



# Diplomado en Bitcoin

*Educación Financiera para la Era Bitcoin*

***Libro de Trabajo para Estudiantes***

Quinta Edición | Julio 2023

*Mi Primer Bitcoin* ha creado este trabajo y lo ha hecho disponible gratuitamente bajo *Creative Commons*.

Este trabajo tiene una licencia

*Creative Commons*

*Atribución-CompartirIgual*

*4.0 Internacional (CC BY-SA 4.0)*

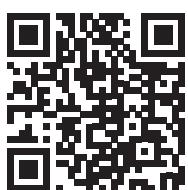
# Diplomado en Bitcoin

*Educación Financiera para la Era Bitcoin*

*Libro de Trabajo para Estudiantes*

Quinta Edición | Julio 2023

PARA DONAR:



bc1qc0h5ddd4ln4z05u55l87cp4umg8eg0jjkhcgvf



## Agradecimientos

El Diplomado en **Bitcoin** ha sido un éxito rotundo y ha crecido más rápido de lo que nadie esperaba. Nos gustaría agradecer a todas las maravillosas personas que nos han traído hasta aquí.

Dalia Platt es la líder del desarrollo del currículo y ha sido la fuerza motriz detrás de nuestro contenido desde el principio. Ella es una estrella. Ha tenido gran ayuda para esta edición de algunos colaboradores increíbles, incluyendo a Alejandro Galán, Jorge Luis Contreras, Hector Alvaro, Reckless Apotheosis, Ernesto Elías de Escuelita **Bitcoin**, Roberto Magana, Reyna Chicas, Arel Edelkamp, Seb Bunney y Zussel Abigail de AmityAge Academy. Greg Foss, Looking Glass Education, Gloriana Solano, Robert Malka, Raul Guirola, Giacomo Zucco, Gerson Martinez, y otros apoyaron las ediciones anteriores. Gerardo Apostolo y Enrique Jubis, con ACTIVA, también aportaron su increíble trabajo.

La historia del Diploma **Bitcoin** comenzó en febrero de 2022 en una reunión en La Pacheco, una escuela pública en San Marcos, El Salvador. Entre los presentes estaban el innovador director de la escuela, Asael Rodriguez, el defensor de la educación en **Bitcoin** y congresista, Rodrigo Ayala, y el constructor de la comunidad para Ibex Mercado, Carlos Toriello, quien invitó a otros bitcoiners, incluyéndome, a visitar la escuela y discutir la educación.

Los primeros estudiantes del Diplomado en **Bitcoin** comenzaron en abril, con el apoyo inicial de Ibex y cientos de donantes individuales. En junio, el primer grupo de 38 estudiantes se graduó en La Pacheco y comenzamos a expandirnos. Con un gran apoyo de nuevos donantes y patrocinadores, incluyendo Bitfinex, alcaldes locales y **Bitcoin** Beach, la matrícula ha continuado más que duplicándose cada diez semanas, una tendencia que nos permitirá llegar a miles de estudiantes en todo el país este año. En febrero de 2023, la entrega del currículo comenzó en Guatemala con planes de llevarlo a muchas más naciones antes de que termine el año, incluyendo Colombia, Honduras, Sudáfrica, Ecuador y Estados Unidos. Las donaciones de esos programas subsidiarán a aún más estudiantes en El Salvador.

El libro de trabajo del Diplomado en **Bitcoin** se ha hecho de código abierto. Está libremente disponible y se ha traducido, impreso y enseñado de forma independiente a comunidades alrededor del mundo, desde Corea del Sur hasta Uruguay.

Mi Primer **Bitcoin** es una organización sin fines de lucro con una única misión: proporcionar educación en **Bitcoin** de calidad, independiente e imparcial, basada en la comunidad a todos en El Salvador lo más rápido posible. Como la primera nación en adoptar **Bitcoin**, El Salvador será un ejemplo para el mundo; nosotros decidimos qué tipo de ejemplo será. Nuestra visión es enseñar a una nación y cambiar el mundo. Sé que suena loco, pero creo que estamos bien encaminados y el Diplomado en **Bitcoin** es una gran parte de eso.

Por un mundo mejor,

*John Dennehy  
Fundador  
Mi Primer Bitcoin*

## Diplomado en Bitcoin

*Un viaje transformador de diez semanas, a través de educación independiente, imparcial, de alta calidad y completamente gratuita.*



Sea lo que sea Bitcoin, la mayoría de la gente aún no entiende de qué se trata esta controvertida e influyente innovación y cómo funciona.

Este es un documental que te ayuda a responder esas preguntas.  
*'The Great Reset'*

Estás a punto de entrar a un mundo completamente nuevo y fascinante. Pero antes, vamos a hacer un pequeño viaje en el tiempo. ¿Alguna vez te has preguntado cómo comenzó todo esto del dinero? ¿Cómo pasamos de intercambiar ovejas y grano a usar monedas, billetes y ahora incluso dinero digital?

Bueno, esa historia es fascinante y es la clave para entender por qué **Bitcoin** es tan revolucionario. Verás, el sistema financiero actual tiene algunas limitaciones. Algunas de estas son complicadas y otras son frustrantes. Pero aquí es donde entra **Bitcoin**, con una propuesta innovadora para abordar estos problemas.

Puede parecer un poco complicado al principio, pero no te preocupes. Como en cualquier objetivo valioso a alcanzar, aprender sobre **Bitcoin** lleva tiempo y concentración. Pero confía en el proceso. Porque, ¿sabes qué? Al final del camino, te espera el premio de entender y apreciar un campo verdaderamente innovador. ¡Esperamos que le saques provecho!

#### *Un Mensaje de Nuestro Fundador*



# Índice

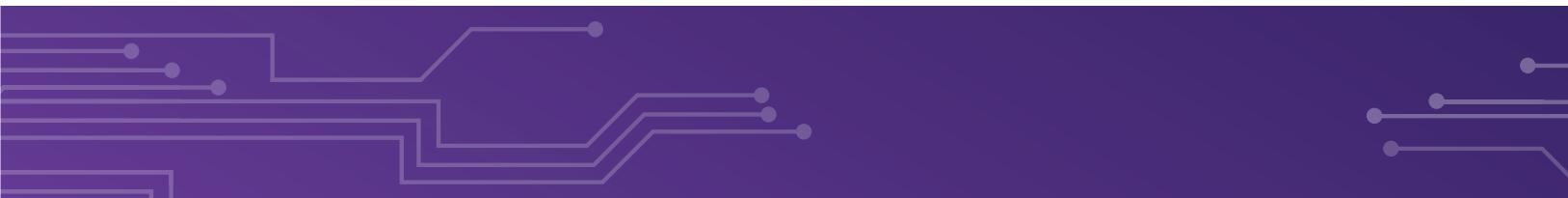
Capítulo #1 - El Poder del Dinero .....	9
1.0 ¿Listo? .....	10
1.1 Discusión en Clase: ¿Qué es el Dinero? .....	10
1.2 El Mundo Limitado: Navegando la Escasez en una Economía en Crecimiento .....	11
1.2.1 Actividad de Clase: Preferencia Temporal .....	11
1.3 Definición de Dinero .....	14
1.3.1 Podemos Usarlo, ¿Pero, Podemos Definirlo? .....	14
1.3.2 Funciones del Dinero .....	16
1.3.3 Características del Dinero .....	28
1.3.4 Tipos de Dinero .....	21
Capítulo #2 - Del Trueque al Bitcoin y los CBDC: Un viaje a través del tiempo .....	25
2.0 Dinero: Un Pasado Tangible, Un Futuro Digital .....	26
2.0.1 Ejercicio en Clase: Juego de Trueque .....	26
2.1 Formas Tempranas de Dinero .....	28
2.2 De las Materias Primas a los Pagarés .....	29
2.3 Transición de Dinero Sólido a Dinero Fiduciario .....	30
2.4 Trazando la Evolución del Dinero Plástico al Digital .....	32
2.5 El Dinero y el Tiempo: Un Enlace Inseparable .....	34
Capítulo #3 - Descubriendo el Lado Oscuro del Dinero Fiduciario .....	37
3.0 Las Mayores Amenazas para tu \$: la Inflación, la Devaluación y la Pérdida de Poder Adquisitivo .....	38
3.1 Desventajas del Sistema Fiat .....	40
3.1.1 Los Efectos de la Inflación: Una Actividad de Subasta .....	40
3.1.2 Ahorrar Dinero en Tiempos Difíciles .....	46
3.1.3 El Valor Temporal del Dinero y su Importancia en el Crecimiento Económico .....	47
3.2 El papel del Banco Central en el Manejo del Dinero .....	48
3.3 La Magia de la Creación de Dinero .....	50
3.3.1 La Banca de Reserva Fraccionaria .....	50
3.3.2 Actividad. Banca con Reserva Fraccionaria .....	52
3.4 Deuda: La Carga que Aplasta a las Clases Media y Baja .....	53
3.4.1 La Toma de Decisiones .....	55



Capítulo #4 - Centralizado vs. Descentralizado: ¿Qué Sistema y Registro es Mejor para Ti? .....	57
4.0 Los Peligros de la Centralización	58
4.1 El Ascenso de una Sociedad Sin Efectivo	58
4.2 Regulaciones Financieras, Censura y Consecuencias Económicas	64
4.2.1 Actividad. Las Consecuencias de la Centralización Digital	66
4.2.2 El Precio del Control	67
4.3 De la Crisis a la Innovación	69
4.3.1 Una Comparación entre las Finanzas Centralizadas y Descentralizadas	69
4.4 Una Herramienta Poderosa para Superar las Limitaciones de la Centralización	70
4.4.1 Las <b>Transacciones</b> son Simplemente Acuerdos para Comerciar	71
4.4.2 Actividad. El Problema de los Generales Bizantinos y la Descentralización	72
4.4.3 Del Valor de la Confianza a la Seguridad de las Reglas	73
4.5 "Desencadenando" el Poder de la Cadena de Bloques	74
4.5.1 La analogía: Un Vehículo Autónomo	74
Capítulo #5 - El Futuro del Dinero Sólido: Introducción al Bitcoin .....	77
5.0 La Revolución Financiera	78
5.1 ¿Qué es <b>bitcoin</b> ? ¿Qué es <b>Bitcoin</b> ?	80
5.1.1 ¿Cuál es la diferencia entre <b>bitcoin</b> y <b>Bitcoin</b> ?	81
5.1.2 ¿Para qué aprender sobre <b>bitcoin</b> si me es imposible pagarla?	81
5.1.3 ¿De qué está hecho el <b>bitcoin</b> ?	82
5.1.4 ¿Cómo recibes <b>bitcoins</b> ?	82
5.1.5 ¿Cómo utilizo por primera vez?	83
5.1.6 ¿Cómo puedo enviar o transferir <b>bitcoin</b> de un monedero a otro?	83
5.1.7 ¿Qué me impide duplicar el mismo <b>bitcoin</b> y enviarlo a varias personas?	83
5.1.8 ¿Cómo ingresan nuevos <b>bitcoins</b> a la red?	84
5.1.9 ¿Se puede apagar o prohibir <b>Bitcoin</b> ?	84
5.2 ¿Quienes son los Protagonistas en el Mundo de <b>Bitcoin</b> ?	85
5.3 Cómo Funciona una <b>Transacción</b> de <b>bitcoin</b> en <b>Bitcoin</b>	87
5.3.1 Actividad: Experimentando las <b>Transacciones</b> en Acción	91

# Índice

5.4 Un Nuevo Enfoque al Dinero	92
5.4.1 ¿Cual es la Mayor Diferencia entre <b>Bitcoin</b> y la Banca Tradicional?	93
5.4.2 Evaluando el Consumo Energético: Bitcoin frente a la Banca y la Minería Tradicionales	94
5.5 ¿Son Seguras las <b>Transacciones</b> de <b>bitcoin</b> ?	95
Capítulo #6 - Carteras de Bitcoin Desbloqueadas: Navegando la Auto-Custodia y la Red Lightning .....	97
6.0 De Novato a Experto: Navegando el Mundo de las Carteras de <b>Bitcoin</b>	98
6.1 Rampas de Acceso y Protección de tu <b>bitcoin</b>	102
6.1.1 Ejercicio de Clase: Dominando la Autocustodia y Usando Monederos con Confianza	103
6.2 On-Chain ( <b>Transacciones</b> en Cadena) vs. Off-Chain ( <b>Transacciones</b> Fuera de Cadena)	104
6.2.1 Una analogía de una <b>Transacción</b> On-chain	105
6.2.2 ¿Cómo Recibo <b>bitcoin</b> on-chain?	106
6.2.3 Ejercicio de Clase: Cómo Enviar <b>bitcoin</b> y Pagar Bienes y Servicios	106
6.3 La <b>Red Lightning</b> - Una Solución para <b>Transacciones</b> Rápidas y Seguras	107
6.3.1 Monederos de la Red Llightning	109
6.3.2 Una <b>Transacción</b> en la <b>Red Lightning</b>	110
6.3.3 Actividad: Carrera de Relevos de Billeteras <b>Lightning</b>	112
6.3.4 Ejercicio de Clase: Demo Interactivo en línea de <b>Lightning</b>	113
Capítulo #7 - Descubriendo la Seguridad de Bitcoin: Las Matemáticas, el Mempool y los UTXO .....	115
7.0 El Problema del Doble Gasto: Entendiendo la Solución de <b>Bitcoin</b>	117
7.1 Funciones y <b>Transacciones</b> : La Cocina de <b>Bitcoin</b>	118
7.2 La "Mempool" o la Piscina de Memoria: El Guardián contra el Doble Gasto	119
7.3 El Papel Crucial del la Criptografía de Claves Públicas	120
7.4 Descifrando la Criptografía Hash	122
7.4.1 Ejercicio de Criptografía	127
7.5 Rastreando la Trayectoria de tu Moneda	128
7.5.1 Ejercicio. Explorando <b>Transacciones</b> No Confirmadas	131



Capítulo #8 - Construyendo la Cadena de Seguridad .....	133
8.0 La Búsqueda en el Jardín Encantado: Una Introducción a la Minería de <b>Bitcoin</b>	135
8.1 La Estructura de Incentivos en Minería. Un Vistazo al ¿ Por qué?	136
8.1.1 El Sistema de Recompensa de Bloques y su Origen	136
8.1.2 El Concepto de "Halving"	137
8.1.3 La Evolución y La Importancia de los "Pools" de Minería	138
8.2 Cadena Inquebrantable: La Dinámica del Hash de Bloque. Un Vistazo al ¿Qué?	139
8.2.1 El Hash del Bloque y el Valor Objetivo	140
8.3 Candidatos a Bloque: Tejiendo Historias Épicas. Un Vistazo al ¿Cómo?	141
8.3.1 Estructurado de un Bloque : Anatomía de un Elemento Vital	142
8.3.2 <b>Transacción</b> Coinbase: Un Premio Especial en la Cadena de Bloques	144
8.4 La Búsqueda del Hash Válido. Un Segundo Vistazo al ¿Cómo?	147
8.5 La Gran Carrera del Hash: ¿Quién Resolverá el Bloque Primero?	149
8.5.1 Actividad Interactiva de Minería	149
8.5.2 Actividad. Proceso de Tramsacciones y Minería en el Modelo UTXO	151
8.6 Diversidad de Direcciones <b>Bitcoin</b> : ¿Por Qué y Para Qué?	151
Capítulo #9 - Descubriendo el Valor Real de <b>Bitcoin</b> : Más Allá de la Superficie .....	153
9.0 ¿Por qué Bitcoin? Una Revolución Financiera y Social	154
9.1 Desmitificando Bitcoin: Mitos y Realidades	154
9.2 ¿Qué le da valor al Bitcoin?	156
9.3 Las Múltiples Dimensiones de Bitcoin	158
9.3.1 El Protocolo Base: Bitcoin Core	158
9.3.2 Ampliando las Fronteras con la Lightning Network	158
9.4 Imaginando un Futuro HiperBitcoinizado	161
Capítulo #10 - De bits a <b>Bitcoin</b> : Ensamblando el Rompecabezas .....	165
10.0 Directrices para la Presentación del Proyecto Final "Mi Primer <b>Bitcoin</b> " y Criterios de Evaluación	166
Recursos Adicionales .....	169
Glosario .....	177



## ¿Por qué ?

## Pensamiento Crítico.

¿Por qué es Bitcoin importante para ti y cómo crees que cambiará a la humanidad?



# Capítulo #1



## El Poder del Dinero

### 1.0 ¿Listo?

1.1 Discusión en Clase: ¿Qué es el Dinero?

1.2 El Mundo Limitado: Navegando la Escasez  
en una Economía en Crecimiento

1.2.1 Actividad de Clase: Preferencia Temporal

1.3 Definición de Dinero

1.3.1 Podemos Usarlo, ¿Pero, Podemos Definirlo?

1.3.2 Funciones del Dinero

1.3.3 Características del Dinero

1.3.4 Tipos de Dinero



## 1.0 ¿Listo?

¡Bienvenido al diplomado de **Bitcoin**! Aquí no solo despejaremos mitos, sino que te brindaremos un conocimiento sólido sobre esta revolucionaria moneda digital. Vamos a profundizar en la tecnología que la sustenta y en cómo tiene el potencial de modificar nuestra relación con el dinero.

Si estás listo para ir más allá de los titulares y sumergirte en el mundo real de **Bitcoin**, este es tu punto de partida ideal.



¡Hola! Soy Satoshi, un asistente interactivo que te ayudará a lo largo del Diplomado en **Bitcoin**. Te daré datos y recomendaciones para que entiendas mejor todo contenido.



### 1.1 Discusión en Clase: ¿Qué es el Dinero?

- Por favor, no te comas todavía el caramelo que tienes sobre la mesa.
- Levanta tu mano si estarías dispuesto a cambiar tu caramelo por un billete de \$5USD.
- Ahora, deja tu mano arriba si todavía estarías dispuesto a hacer el cambio de tu caramelo por un billete de \$5 de Monopolio. Y, ¿que tal si te ofrezco \$100,000,000,000,000 de dólares de Zimbabwe?
- ¿Qué hace que un billete sea tan deseable y otro tan inútil?
- ¿Qué confiere al dinero su "valor"?



La única diferencia entre estos billetes es tu creencia de que una tiene más valor que la otra.

- ¿De dónde viene el dinero y quién decide cuánto se imprime?
- ¿Por qué no imprimir más dinero y repartirlo entre todos por igual?
- ¿Está el dinero respaldado por el oro? ¿O por cualquier otra mercancía?
- ¿Cuánta gente sigue utilizando dinero en efectivo?



## Capítulo #1

### 1.2 El Mundo Limitado: Navegando la Escasez en una Economía en Crecimiento

#### 1.2.1 Actividad de Clase: Preferencia Temporal

**Actividad de Clase.** ¡Bienvenido a la Actividad del Marshmallow! Aquí aprenderás sobre toma de decisiones, espera y la incertidumbre.

Te darán un marshmallow y tendrás la opción de comerlo ya o esperar para tener la posibilidad de ganar uno más. Si esperas, se lanzará una moneda: cara te permite elegir entre tazas o bolsas que podrían contener un segundo marshmallow; sello significa que tendrás que seguir esperando. Al final, hablaremos de las emociones que sentiste y cómo se relacionan con decisiones en la vida real.

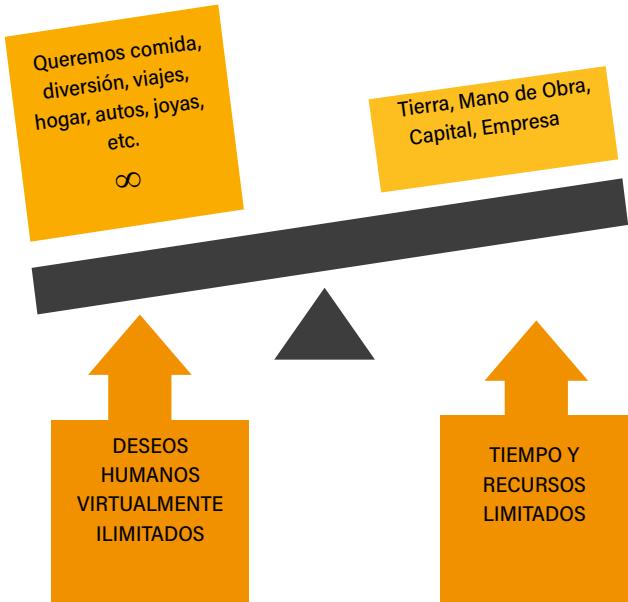
¡Recuerda, es una lección de vida disfrazada con marshmallows! ¡Disfrútala!



Ahora imagina que estás varado en un desierto y solo te queda una botella de agua. Tienes sed y estás desesperado por tomar un traguito, pero también sabes que necesitarás el agua para sobrevivir hasta que puedas encontrar más. Este es un ejemplo clásico de **escasez**: solo tienes una **cantidad limitada** de un **recurso** (agua) y debes tomar una decisión sobre cómo usarlo.

En esta situación, puedes decidir racionarla y tomar pequeños sorbos durante un período de tiempo más largo, para hacer que dure lo más posible. Alternativamente, puedes decidir beber tanto como puedas de una sola vez, esperando que el estallido de hidratación te dé la energía que necesitas para encontrar más agua. Independientemente de la elección que hagas, te enfrentas a una decisión difícil.

En este caso, la elección es entre saciar tu sed inmediata y conservar el agua para más tarde. Este concepto de escasez se aplica a todo tipo de recursos, no solo al agua. Ya sea dinero, tiempo o incluso amor y atención, constantemente nos enfrentamos a decisiones sobre cómo asignar nuestros recursos limitados. Buscamos satisfacer **necesidades** tales como la alimentación, diversión, viajes, hogar, autos, joyas, entre otras.



La escasez nos obliga a sopesar los pros y los contras de cómo usamos nuestros recursos y hacer compensaciones.

Los deseos humanos son virtualmente ilimitados, mientras que los recursos limitados incluyen tierra, trabajo, capital y empresa, además del tiempo.

- Existen dos tipos de escasez: la escasez creada por el hombre y la escasez natural.

○ La escasez creada por el hombre, también conocida como escasez centralizada, incluye cosas como bolsos de diseñador de edición limitada, cartas deportivas raras y piezas de arte numeradas. Estos productos pueden replicarse o falsificarse fácilmente.

○ La escasez natural, también conocida como escasez descentralizada, incluye cosas como sal, conchas y metales preciosos como el oro. Estos recursos son más difíciles de replicar o falsificar.

- La principal diferencia entre las dos es el control. La escasez centralizada está controlada por una sola entidad, como una empresa o gobierno, mientras que la escasez descentralizada no está controlada por nadie.

El control centralizado de recursos esenciales como el agua puede causar una escasez desproporcionada que afecta a las comunidades de bajos ingresos. Cuando entidades privadas o gubernamentales limitan el acceso a estos recursos, pueden surgir situaciones de monopolio, permitiendo a estas entidades subir los precios o limitar aún más el acceso. Las comunidades pobres, al tener un acceso restringido a estos recursos vitales, experimentan no solo un impacto negativo en su salud y bienestar, sino también un refuerzo de las condiciones de pobreza existentes. Pueden enfrentar precios más altos por el agua o tener que recorrer grandes distancias para conseguirla, lo que a su vez limita el tiempo que podrían dedicar a actividades generadoras de ingresos o educativas. Esto perpetúa un ciclo de pobreza y privación, mostrando cómo la centralización y la escasez pueden tener efectos negativos en las comunidades más vulnerables.

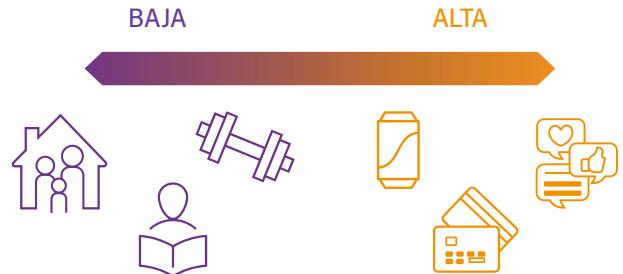
Entender la escasez nos ayuda a tomar decisiones, ya que debemos elegir entre beneficios ahora o en el futuro. Estas elecciones nos guían hacia nuestros objetivos.



# Capítulo #1



*La (alta) preferencia temporal* se refiere a la idea de que las personas generalmente prefieren tener algo AHORA en lugar de más tarde.



Por ejemplo, digamos que tienes la opción de recibir \$100 hoy o \$150 en un año. Si tienes una *alta* preferencia temporal, es posible que elijas recibir los \$100 hoy, porque valoras la satisfacción inmediata de tener el dinero ahora más que el beneficio potencial de esperar \$50 adicionales en un año. Por otro lado, si tienes una *baja* preferencia temporal, podrías estar dispuesto a esperar la recompensa más grande en el futuro, porque te preocupa menos la gratificación inmediata y estás más enfocado en la planificación a largo plazo.

- ¿Se te ocurren ejemplos de la vida real en los que una alta preferencia temporal podría ser perjudicial y una baja preferencia temporal podría ser beneficiosa?
- ¿Cuáles son las posibles consecuencias de elegir una preferencia temporal alta en lugar de una preferencia temporal baja?

En el contexto del ejemplo del desierto, esto significa que es posible que estés más inclinado a beber toda el agua de inmediato, incluso si eso significa que no tendrás nada para más tarde. Esto se debe a que la sed que sientes en este momento es más urgente que la posible sed que podrías sentir en el futuro. Por otro lado, si decides racionar el agua y beberla lentamente con el tiempo, estás demostrando una baja preferencia por el tiempo. Esto significa que estás dispuesto a esperar para satisfacer tu sed para tener una mayor oportunidad de supervivencia a largo plazo.

El concepto de *costo de oportunidad* está estrechamente relacionado con la idea de *escasez* y *preferencia temporal*.



El *costo de oportunidad* se refiere al valor de la mejor alternativa que renuncias cuando tomas una decisión.

## La Decisión de Hoy



Comprar un batido de fresa de \$7 USD.

## AHORA



Gastar \$7 USD de otra manera.



## DESPUÉS



Beneficiándose de \$7 USD ahorrados regularmente.

Toda decisión implica compensaciones. El costo de oportunidad de beber toda el agua de inmediato en el ejemplo del desierto es el beneficio de supervivencia que habrías obtenido al racionar el agua y usarla durante un período más prolongado.

Digamos que decides racionar el agua y tomar pequeños sorbos durante un período más prolongado. Como resultado, tienes la energía e hidratación que necesitas para buscar más agua. Como resultado, te encuentras con un cactus que tiene una pequeña cantidad de agua adentro. No es mucho, pero es suficiente para saciar tu sed por el momento (y mantenerte vivo por más tiempo). Si hubieras decidido beber toda tu agua de una vez, es posible que no hubieras tenido la energía para buscar más agua y encontrar el cactus.

En este caso, el *costo de oportunidad* de beber toda tu agua de una vez habría sido la oportunidad de encontrar el cactus y obtener más hidratación. Este ejemplo ilustra cómo el costo de oportunidad no solo implica la compensación inmediata entre dos opciones, sino también las posibles oportunidades futuras que se pueden ganar o perder como resultado de nuestras elecciones. Nuestra disposición a renunciar a una recompensa mayor en el futuro a cambio de una recompensa menor ahora está influenciada por nuestra preferencia temporal, o cuánto valoramos la gratificación inmediata frente a la planificación a largo plazo.

Las corporaciones, los gobiernos y las sociedades también tienen que tomar decisiones.

CORPORACIONES	GOBIERNOS / SOCIEDADES
Despedir a 200 Empleados o Congelar Salarios a 600 Empleados	Construir una Nueva Autopista o. Aumentar los Salarios de los Maestros
Solicitar un Préstamo o Atraer a más Accionistas	Financiar la Investigación de Tratamiento del Cáncer o Invertir en Energía Limpia

## 1.3 Definición de Dinero

### 1.3.1 Podemos Usarlo, ¿Pero, Podemos Definirlo?

¿Alguna vez has pensado qué es realmente el dinero? ¿Te has preguntado qué hace que el dinero sea, buen dinero? La mayoría de nosotros sabemos cómo utilizarlo, pero no muchos entendemos de dónde viene o cómo funciona.

El dinero es un medio esencial para intercambiar bienes y servicios, ya que representa su valor de manera fácilmente transferible. El dinero, que puede adoptar diversas formas como billetes de papel, monedas de metal o pagos electrónicos, es emitido y controlado generalmente por gobiernos u otras autoridades.

El dinero, ya sea físico o digital, actúa como un lenguaje universal. Cruza fronteras, supera barreras lingüísticas y une diversas culturas. Imagina estar en una ciudad totalmente desconocida, en un país donde no entiendes el lenguaje ni las costumbres. Aun así, puedes entrar a una tienda, seleccionar un artículo y "comunicarte" a través del lenguaje del dinero. Al pagar con moneda local o tarjeta de crédito, has llevado a cabo una **transacción** internacional sin necesidad de palabras. El dinero es un puente que facilita la conexión y el intercambio entre distintos mundos.



# Capítulo #1

El dinero es un pacto colectivo, un acuerdo invisible que nos libera de la complejidad del trueque, evitando la tediosa búsqueda de la coincidencia de deseos. Imagina una realidad en la que aceptamos el chocolate como una forma válida de pago. De repente, las deliciosas tabletas de cacao se convierten en billetes dulces que circulan por nuestras manos.



Sin embargo, aunque el chocolate puede ofrecer satisfacción instantánea, tiene sus limitaciones como divisa. Imagina un verano caliente, los "billetes" de chocolate se derriten en nuestros bolsillos, desvaneciéndose como una economía en crisis. Así, aunque el chocolate puede ser una delicia, su utilidad como dinero puede ser tan efímera como su estado sólido bajo el sol.

Como dijo el economista francés Jean-Baptiste Say:

*"El dinero no desempeña más que una función momentánea en un intercambio; y cuando la transacción se cierra finalmente, siempre se encontrará que se ha cambiado una clase de mercancía por otra."*

En otras palabras, el dinero en sí no tiene el poder de satisfacer los deseos humanos. Es sólo una herramienta que nos permite intercambiar una mercancía por otra.



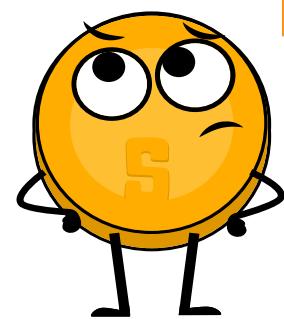
Una **transacción** es un intercambio o transferencia de bienes y servicios. Es una forma de acordar valor entre dos o más partes.

Existen muchos tipos de **transacciones**, que van desde intercambios simples (como comprar un sándwich en una tienda) hasta **transacciones** financieras más complejas (como comprar una casa o invertir en acciones o bonos). Las **transacciones** se pueden realizar en persona, por teléfono, en línea o por otros medios, y pueden involucrar a una amplia gama de partes, incluidas personas, empresas e instituciones financieras.



Sin dinero,  
¿cómo de fácil o  
factible sería este  
intercambio?

- ¿Cambiarías una vaca por 1.000.000 fresas?
- ¿O por 600.000 fresas?
- ¿Qué tal 50.000?



# El Poder del Dinero



El dinero es como un mensajero que ayuda a intercambiar cosas como bienes y servicios. Representa su valor para hacer más fácil el trato, pero no es lo mismo que el valor de esas cosas. Es solo una forma de mover ese valor de un lugar a otro.

En resumen, el dinero:

- Facilita el comercio porque todos lo aceptan como pago final.
- Nos permite medir el valor de y hacer comparaciones entre diferentes bienes y servicios.
- Reduce nuestra preferencia temporal, permitiéndonos ahorrar y gastar en el futuro.



¡Mira este breve vídeo!  
Qué es el Dinero?



## 1.3.2 Funciones del Dinero

Cuando se trata de comprar y vender bienes y servicios, el dinero es la pieza clave. Tiene varios trabajos importantes, como:

- **Facilitar intercambios:** Con dinero, no tienes que encontrar a alguien que quiera exactamente lo que tienes para intercambiar. En su lugar, puedes usar dinero para comprar y vender cualquier cosa que desees. Esto hace que el comercio sea mucho más conveniente y eficiente.

### Medio de Intercambio



- **Ser una unidad de cuenta:** El dinero proporciona un estándar universal de valor que permite a las personas expresar y comparar el precio de diferentes bienes y servicios. Esto permite un mercado más eficiente y transparente, donde las personas pueden tomar decisiones informadas sobre qué comprar y vender.

- Consideralo así: al querer comprar un carro nuevo, puedes comparar precios entre concesionarios y tomar una decisión informada basándote en su valor en dólares. Sin una unidad de cuenta, tendrías que evaluar el valor de un carro respecto a otro usando otras medidas, como la cantidad de vacas a intercambiar o el tiempo de fabricación.



# Capítulo #1



## Unidad de Cuenta

Los consumidores conocen el valor de algo cuando se le asigna un precio (valor monetario).

\$29.00



\$129.00



- **Ser una reserva de valor:** El dinero debe mantener su valor con el tiempo, lo que lo hace útil como una forma de ahorrar e invertir el valor del trabajo humano. Esto permite que las personas usen el dinero para planificar el futuro, para pedir prestado y prestar dinero.



*¿Cuál es su reserva de valor?*

	(USD)	Gold (USD)	USD (EUR)
14 de marzo de 2019	\$3,846	\$1,293	€0.8817
14 de marzo de 2020	\$5,258	\$1,529	€0.90056
Ganancia / Pérdida	+36.71%	+18.25%	+2.14%

Entonces, la próxima vez que estés ahorrando para algo especial, recuerda que el dinero es más que solo una forma de pagar por las cosas, es una herramienta para ayudarte a planificar e invertir en tu futuro.

Estas tres funciones son las que permiten que las economías se vuelvan complejas y dinámicas. Sin dinero, sería mucho más difícil comprar y vender bienes y servicios, y nuestra economía sería mucho menos desarrollada.

*Ejercicio de Clase.* ¿Cuál es la función de dinero más evidente en cada ejemplo?

1. Roby decide ahorrar una parte de su sueldo semanal para poder comprar un gato.
2. Jim compra dos porciones de pizza por \$8.30 en Ray's Pizza.
3. Marc no puede decidir si comprar entradas para un juego de béisbol por \$75 USD o un pase para esquiar por \$95 USD.

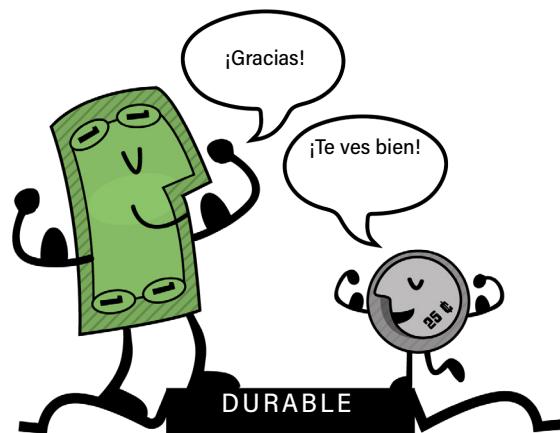
# El Poder del Dinero

## 1.3.3 Características del Dinero

Con el tiempo, la gente se ha dado cuenta de que el dinero debe poseer ciertas cualidades para ser eficaz como medio de intercambio. Estas características incluyen durabilidad, portabilidad, divisibilidad, intercambiabilidad, escasez y aceptabilidad.

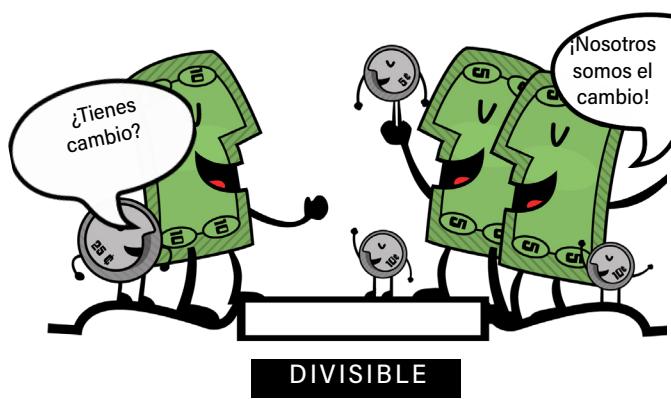
- La **durabilidad** se refiere a la capacidad del dinero para resistir el deterioro físico y perdurar en el tiempo. Esto garantiza que el dinero pueda circular en la economía en un estado aceptable y reconocible.

El oro es un material duradero que puede resistir el desgaste, lo que lo convierte en una buena representación de la característica de durabilidad del dinero.



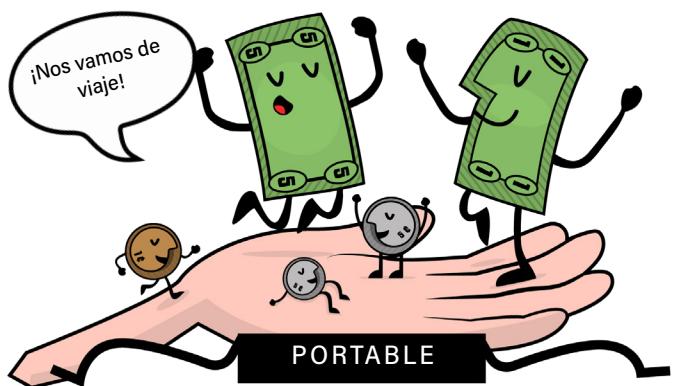
- La **divisibilidad** se refiere a la capacidad del dinero de dividirse en unidades más pequeñas, de modo que la gente pueda utilizarlo para hacer compras de distintos importes.

Los billetes de papel pueden dividirse fácilmente en denominaciones más pequeñas, lo que los convierte en una buena representación de la característica de divisibilidad del dinero.



- La **portabilidad** se refiere a la facilidad con la que el dinero puede transportarse y llevarse de un lado a otro. Esto permite que la gente utilice el dinero para comprar y vender bienes y servicios sin dificultad.

Las tarjetas de crédito son portátiles, ya que pueden llevarse fácilmente en una billetera o en un bolsillo, lo que las convierte en una buena representación de la característica de portabilidad del dinero.





## Capítulo #1

- **La aceptabilidad** se refiere a la aceptación generalizada del dinero como forma de pago, de modo que la gente pueda utilizarlo para comprar y vender bienes y servicios con confianza.

El dólar estadounidense es ampliamente utilizado como forma de pago, lo que lo convierte en una buena representación de la característica de aceptabilidad del dinero.



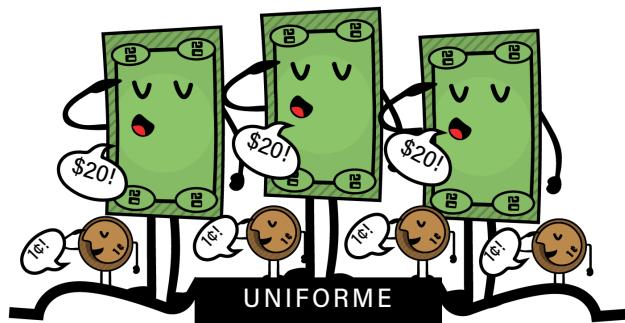
- La **escasez** se refiere a la oferta limitada de dinero, que ayuda a mantener su valor. Evita que la gente tenga que gastar más dinero para comprar la misma cantidad de bienes.

Las estampillas de colección, especialmente aquellas que son raras y valiosas, pueden ser una buena forma de dinero porque son escasas y pueden valorizarse con el tiempo. Los coleccionistas de estampillas suelen utilizarlas como forma de invertir su patrimonio y diversificar su cartera.



- La **uniformidad** se refiere a la intercambiabilidad del dinero, de modo que una unidad de dinero sea equivalente a otra unidad del mismo valor.

Las monedas de cobre son uniformes en tamaño y peso, lo que las convierte en una buena representación de la característica de uniformidad del dinero. - Un centavo siempre es un centavo, y un euro es un euro.



En general, estas características hacen del dinero una herramienta útil y eficiente para facilitar el intercambio y el comercio, siendo esenciales para el desarrollo y estabilidad económica.

# El Poder del Dinero

**Ejercicio de Clase.** Los distintos activos tienen diversas propiedades que les permiten cumplir las funciones del dinero en diferentes medidas. Lo que se utiliza como dinero en la sociedad es decidido por su estabilidad, rareza, divisibilidad, transferibilidad y aceptación como medio de cambio.

Esta actividad de clase nos ayudará a entender cómo diferentes elementos se adaptan a las características específicas del dinero. Calificaremos cada elemento en una escala del 0 al 10 en cada característica. Sumaremos las calificaciones de cada elemento para determinar cuál sería más idóneo como dinero.

[0 = Inapropiado; 5= Satisfactorio; 10 = Óptimo]

Por ahora, deja la columna de **Bitcoin** en blanco; la completaremos más adelante en el curso.

Utiliza las siguientes preguntas para evaluar cómo los distintos elementos de la tabla cumplen con las características del dinero:

- **Durabilidad:** ¿Resiste el dinero el desgaste y deterioro a lo largo del tiempo?
- **Portabilidad:** ¿Es el dinero fácilmente transportable y utilizable en distintas ubicaciones?
- **Uniformidad:** ¿Es el dinero intercambiable con otras formas monetarias?
- **Aceptabilidad:** ¿Se acepta ampliamente el dinero como medio de pago?
- **Escasez:** ¿Es el dinero escaso y no excesivamente abundante?
- **Divisibilidad:** ¿Puede dividirse el dinero en unidades más pequeñas para realizar **transacciones**?

Características de un buen dinero	 Vacas	 Cigarrillos	 Diamantes	 Euros	 Bitcoin
<b>DURABLE</b>					
<b>PORTABLE</b>					
<b>UNIFORME</b>					
<b>ACEPTABLE</b>					
<b>ESCASO</b>					
<b>DIVISIBLE</b>					
<b>TOTAL</b>					



## Capítulo #1

### 1.3.4 Tipos de Dinero

El dinero puede dividirse en dos categorías principales: **físico y digital**.

El **dinero físico** incluye:

- **El dinero mercancía**, que es un objeto físico con valor intrínseco y ampliamente aceptado como medio de cambio. Por ejemplo, el oro y la plata.
- **El dinero representativo**, que representa un derecho sobre un bien físico.
- **El dinero fiduciario**, que son los billetes de papel y monedas emitidos por los gobiernos y aceptados como medio de cambio.

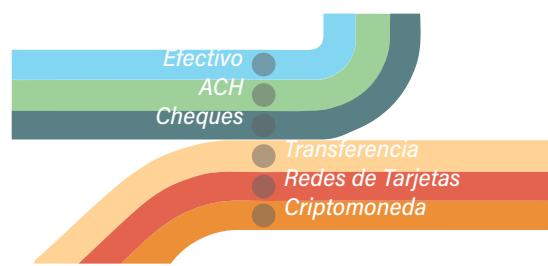


El **dinero digital**, por otro lado, puede utilizarse para **transacciones** en línea e incluye monedas electrónicas, monedas estables y criptodivisas.



Las **monedas electrónicas** son versiones digitales del dinero físico, como dólares o euros, y pueden utilizarse para comprar y vender cosas en línea a través de **redes o canales de pago digitales**.

Las **redes de pago** son la infraestructura que permite el movimiento de monedas electrónicas y otros activos digitales de un lugar a otro. Sin embargo, en el sistema financiero tradicional, siempre hay un intermediario, como un banco o una institución financiera, que cobra una comisión y tiene autoridad para aceptar, cancelar, revertir o retrasar las **transacciones**.



# El Poder del Dinero

Dentro del sistema financiero intermedio, hay una variedad de **canales de pago digitales** a nuestra disposición. Algunos de los más prominentes son las redes de tarjetas de crédito y débito que facilitan el traspaso de fondos entre entidades financieras y comerciantes al realizar compras. Asimismo, los **billeteras electrónicas (wallets)** se presentan como cuentas virtuales que permiten a los usuarios almacenar, administrar sus divisas digitales y realizar pagos transfiriendo recursos a las cuentas de los beneficiarios.



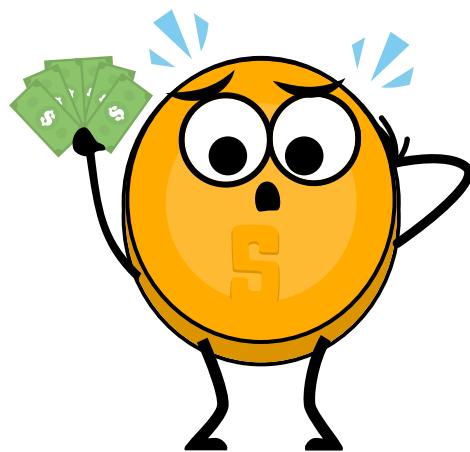
**Las monedas digitales del banco central (CBDC)** son versiones digitales de la moneda fiduciaria de un país, emitidas y respaldadas por el banco central, siendo intermediadas por el gobierno. Las CBDC no son criptomonedas, ya que son emitidas por una autoridad central y no utilizan canales de pago descentralizados.



Las **criptomonedas** son una forma de dinero digital que utiliza **criptografía** para asegurar las **transacciones** y controlar la creación de nuevas unidades. Aunque suelen operar en **redes descentralizadas**, no todas son completamente descentralizadas. Por ejemplo, **Bitcoin** funciona en una red sin control central, mientras que Ripple está gestionada por una organización específica. En estos casos, las **transacciones** podrían ser descentralizadas, pero la toma de decisiones sobre la moneda aún podría estar en manos de una entidad central.

- Las **monedas estables** son **criptomonedas** que mantienen su valor en relación con un activo estable, "como el dólar". Algunas dependen de un intermediario, como un banco, mientras que otras funcionan de forma autónoma y descentralizada.

En última instancia, una moneda que opera sin intermediarios puede ser más eficaz y beneficiosa para la sociedad en su conjunto, ya que impide que unos pocos tengan control sobre la oferta de dinero y acumulen poder desmedido. Sin embargo, el desafío histórico ha sido diseñar tal moneda que permita **transacciones** seguras sin necesidad de una confianza mutua entre las partes. La solución a este reto sería una moneda similar a Internet, en la que el control sea distribuido y nadie posea la totalidad de este. Para lograr esto, incluso las entidades más poderosas tendrían que estar dispuestas a compartir el control en beneficio de todos.





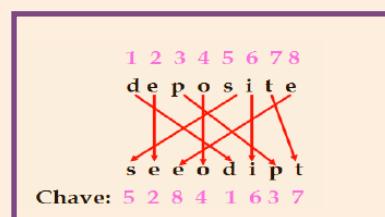
# Capítulo #1



**Nota:** No te preocupes si no entiendes algunos de los términos que usamos en este momento. Los vamos a definir y explicar más adelante. Lo importante ahora es empezar a familiarizarte con ellos.



- **Cifrado o Criptografía:** Un tipo de matemática que hace seguras las **transacciones** en línea.
- **Descentralización:** En el contexto de una red, este término significa que no hay una sola entidad, como una empresa o gobierno, que tenga control total sobre toda la red. En el caso de una criptomoneda, está controlada y mantenida por una comunidad de usuarios, en lugar de una autoridad centralizada.
- **Transacción Digital:** Es el proceso de intercambiar dinero, bienes o servicios a través de medios electrónicos, como aplicaciones de pago o plataformas en línea, en lugar de usar efectivo o métodos de pago físicos.
- **Wallet o Billetera Digital:** Un lugar seguro en tu computadora o en línea para guardar tus criptomonedas.





# Capítulo #2

## Del Trueque al **Bitcoin** y los CBDC: Un Viaje a Través del Tiempo

2.0 Dinero: Un Pasado Tangible, Un Futuro Digital

    2.0.1 Actividad del Dinero (3 Rondas)

2.1 Formas Tempranas de Dinero

2.2 De las Materias Primas a los IOU's

2.3 Transición de Dinero Sólido a Dinero Fiduciario

2.4 Trazando la Evolución del Dinero Plástico al Digital

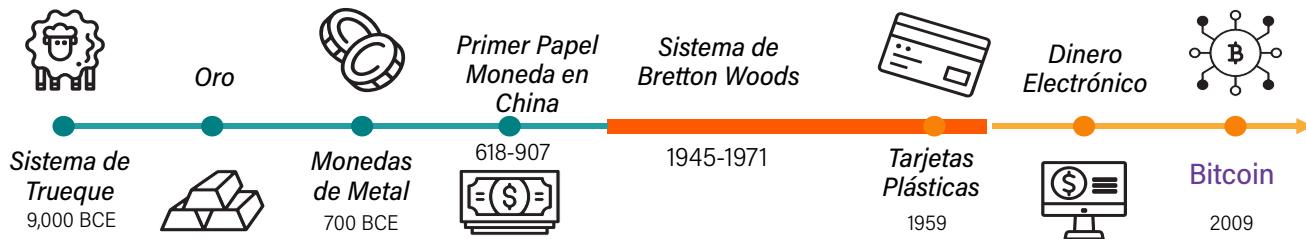
2.5 El Dinero y el Tiempo: Un Enlace Inseparable

# Del Trueque al BTC y los CBDC: Un Viaje a Través del Tiempo

## 2.0 Dinero: Un Pasado Tangible, Un Futuro Digital

El concepto de dinero ha evolucionado. En su forma primitiva, el dinero se utilizaba para facilitar el comercio y el intercambio de bienes y servicios.

- En las civilizaciones antiguas, la humanidad recurrió al trueque, un sistema de intercambio directo de bienes y servicios sin utilizar un medio de cambio.
- Más tarde, se introdujeron las monedas de metal y el papel moneda como formas más convenientes de dinero, abriendo el camino a los sofisticados sistemas financieros que tenemos hoy en día.



A lo largo de este capítulo experimentaremos de primera mano la evolución del dinero. Rastrearemos sus orígenes y observaremos cómo ha cambiado y se ha adaptado a lo largo de la historia.

### 2.0.1 Actividad del Dinero (3 Rondas)

#### ● Ronda #1 - Trueque

Es en el año 6000 a. C. Ni hace falta decir que el dinero, tal y como lo conocemos, no se ha inventado. Te encuentras en Mesopotamia e intercambias directamente bienes y servicios entre unos y otros mediante el trueque.

Tu profesor te ha dado un papelito. Tu objetivo es intercambiar lo que "tienes" por lo que "quieres" en un juego mercantil a lo largo de la historia. Escribe tu nombre en la parte superior del papel con letra pequeña y legible.

- Corta tu hoja por la línea discontinua. Tu objetivo es intercambiar tu "tengo" tantas veces como necesites para conseguir finalmente tu "quiero" original. No puedes cambiar tu "quiero" original. Dispondrás de 5 minutos para cumplir el objetivo de este ejercicio.
- Cuando tu nuevo "tengo" coincida con tu "quiero" original, vuelve a tu asiento. Una vez transcurrido el tiempo, si no has encontrado un compañero de intercambio, vuelve a tu asiento de todos modos.



Levanta la mano si has conseguido lo que querías después de un intercambio. ¿Dos? ¿Tres?



## Capítulo #2



Como nota al margen, muchas empresas siguen aceptando **pagos no monetarios** por sus servicios, y los gobiernos tratan estas **transacciones** de trueque igual que las **transacciones** monetarias a efectos de declaración de impuestos.

### Preguntas. Discute en clase

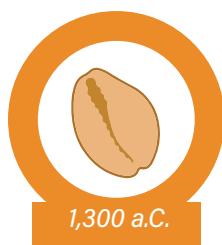
- ¿Por qué algunos lograron encontrar un socio comercial y otros no?
- ¿Cuáles son las ventajas del trueque?
- Basándote en tu experiencia con este ejercicio, ¿cuáles son los inconvenientes de utilizar el trueque?

Ahora te encuentras en la costa occidental de África en el siglo XIV a.C. En esta época, las prácticas de trueque son complicadas e insatisfactorias. Sin embargo, a medida que la sociedad evoluciona, la gente sigue buscando formas más eficaces y eficientes de intercambiar bienes y servicios.

### ● Ronda #2 - Dinero Mercancía

Seguimos viajando a través del tiempo. Nuestra civilización se ha avisado un poco y ha encontrado la forma de resolver ciertos problemas. Tu profesor te ha dado macarrones en representación del dinero de la época. Vuelve a conseguir tu "quiero" negociando su precio en macarrones.

### Conchas de Caracol a Monedas



1,300 a.C.



1,000 a.C.



687 a.C.

#### DATO CURIOSO

Las conchas de caracol eran aceptadas como moneda de curso legal en algunas partes de África hasta el siglo XX.

1,300 a.C.

Las conchas de caracol son la forma predominante de pago en la mayoría de Asia, África, Oceanía y algunas partes de Europa.

1,000 a.C.

La dinastía Zhou Occidental de China comienza a usar monedas de metal.

687 a.C.

El rey Alyates de Lidia (actual Turquía) ordena acuñar las primeras monedas de metal en el mundo occidental.

Estas proto-monedas eran de forma ovalada, estaban hechas de "electrum" (una aleación de oro/plata) y tenían un diseño en un solo lado.

# Del Trueque al BTC y los CBDC: Un Viaje a Través del Tiempo

- ¿Por qué consideramos los macarrones mercancía dinero?
- ¿Cómo conseguimos ahora las cosas que queremos? Supongamos que:
- ¿Fue más fácil la ronda de los macarrones?
- ¿Por qué crees que el dinero ha sustituido a las mercancías?
- ¿En qué sentido es más eficaz utilizar dinero mercancía que el trueque?
- ¿Cuáles son los inconvenientes de utilizar macarrones como dinero?

¿Qué crees que ocurrió cuando España empezó a traer de vuelta a su comunidad barcos cargados de macarrones (oro y plata de las Américas de vuelta a España)?

## 2.1 Formas Tempranas de Dinero



La palabra "salario" proviene del latín "salarium," que originalmente se refería al pago en sal que recibían los soldados romanos por sus servicios.



Mira este breve video para conocer los orígenes del dinero  
"¿Quién inventó el dinero?"

“ ”



En todo sistema de trueque, se enfrenta un desafío llamado la *doble coincidencia de deseos*. Este fenómeno se refiere a la necesidad de que las personas encuentren a alguien que no solo tenga lo que ellos buscan, sino que también desee lo que ellos tienen para ofrecer. *Esta necesidad puede hacer que el trueque sea complejo y a veces ineficiente.*



Te daré zapatos a cambio de tu trigo.

No necesito zapatos. Necesito ropa.

Yo quiero zapatos pero no tengo trigo.

En las economías basadas en el **trueque**, las personas intercambian bienes y servicios según su valor relativo. Sin embargo, este sistema es ineficiente y complicado de manejar, especialmente en sociedades más complejas.



## Capítulo #2

Supongamos que:

- Joseph quiere cambiar su plátano por el coco de Yael.
- Pero Yael sólo quiere cambiar su coco por el mango de Tammy.
- Tammy sólo quiere cambiar su mango por el plátano de Joseph.
- Están atrapados en un ciclo interminable de intercambio de frutas sin que se dé la doble coincidencia de deseos.
- Joseph sugiere que intercambien sus frutas por un refresco bien frío, pero en la isla definitivamente no hay refrescos fríos.
- Deciden sentarse en la playa y disfrutar de sus frutas en silencio.

### *Por qué se Inventó el Dinero*

Lo siento, no tengo  
nada más pequeño.



Utilizar una **unidad de cuenta común**, como un "refresco", hace que el intercambio y el comercio sean mucho más eficientes. En la antigüedad, las personas empezaron utilizando granos, sal, conchas y otros objetos que tenían valor en su sociedad como **medios de intercambio**.



Analizaremos un video basado en el libro de Jacob Goldstein, que recorre la historia y evolución del dinero. El autor nos muestra cómo nuestra visión sobre el dinero ha cambiado a lo largo del tiempo. Goldstein sostiene que el dinero no es solo una herramienta para medir el valor y facilitar el comercio, sino que su definición se reinventa constantemente para satisfacer las necesidades cambiantes de la sociedad.

### **2.2 De las Materias Primas a los Pagarés**

Conforme una comunidad se involucra más en actividades comerciales, se enfrenta a las limitaciones del trueque y el **dinero mercancía** como medios de intercambio. El dinero mercancía, como los metales preciosos, cereales o ganado, ofrecía ciertas ventajas al tener valor intrínseco, pero también planteaba desafíos en términos de divisibilidad, durabilidad y facilidad de transporte. Por esta razón, la sociedad tiende a evolucionar y adoptar el uso de monedas metálicas como forma de dinero, ya que estas resuelven muchos de los problemas asociados con el dinero mercancía.



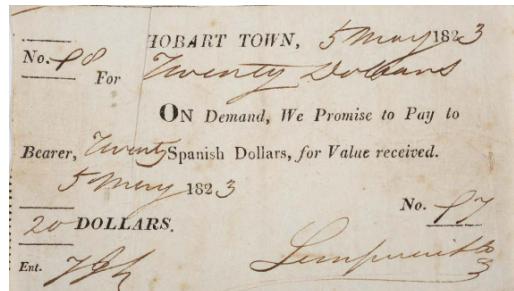
Estas monedas metálicas están hechas de materiales valiosos, como oro y plata, y sirven como medio de intercambio y unidad de cuenta para facilitar el comercio de bienes y servicios; se les denomina **dinero mercancía**.

# Del Trueque al BTC y los CBDC: Un Viaje a Través del Tiempo

Pese a su aparente utilidad, las **monedas metálicas** generan ciertas dificultades. Son pesadas y complicadas de manejar en operaciones grandes y, por si fuera poco, detectas que algunas personas explotan el sistema, fundiendo y mezclando dichas monedas con metales menos valiosos para multiplicar sus beneficios. Esto causa un incremento en los precios de bienes y servicios y sembrar desconfianza en el sistema monetario.

Para abordar estos desafíos, una comunidad podría optar por usar **papel moneda** como un medio tangible de intercambio. Esta forma de dinero, con raíces en la antigua China en el siglo X, se convierte en un recurso de intercambio mucho más práctico y conveniente. Durante los siglos XVII y XIX, el valor del papel moneda se respaldaba por reservas de oro y otros metales preciosos que podían canjearse a pedido. De esta manera, la comunidad tendría acceso a una forma de dinero que no solo es más fácil de manejar y transferir, sino que también conserva la seguridad y el valor inherentes a los metales preciosos.

## Recibo Pagable Exigible a Demanda



## 2.3 Transición de Dinero Sólido a Dinero Fiduciario: El inicio del retroceso

### ● Ronda #3- La Transición

Es el siglo XVII en Suecia, la gente confía en los bancos para proteger sus bienes máspreciados, como el oro. No obstante, empiezan a surgir irregularidades: algunos bancos emiten más recibos de papel que el oro que tienen en sus bóvedas, creando más dinero del que efectivamente respaldan. Esta práctica, además de ser deshonesta, permite a esos banqueros acumular enormes cantidades de riqueza.

**Roles:** Tú serás un depositante, un orfebre o una empresa buscando un préstamo. Usaremos macarrón como oro y notas de papel como promesas de pago (IOUs).

### Paso 1: Intercambio Directo

Depositantes: Dan su macarrón a los orfebres.

Orfebres: Dan un IOU al depositante como recibo del macarrón.

Solo quien tenga el IOU original puede recuperar su macarrón.



### Paso 2: IOUs Transferibles

Ahora puedes dar tu IOU a otra persona.

Cualquier persona con el IOU puede ir al orfebre y reclamar el macarrón.

### Paso 3: Reserva Fraccional (Volveremos a este concepto en el capítulo 3)

Los orfebres emiten más IOUs de los que tienen macarrón.

Ofrecen préstamos con intereses a empresas usando nuevos IOUs.

**El Riesgo:** Si muchos van a reclamar su macarrón al mismo tiempo, el orfebre podría no tener suficiente. Esto se llama una corrida bancaria.



## Capítulo #2



Comienzan a aparecer las *desventajas de esta centralización*, incluyendo el consumo irresponsable, un *aumento de la deuda* y la manipulación económica. La confianza en el sistema bancario comienza a desmoronarse cuando el pueblo se da cuenta de que los números en sus recibos no siempre equivalen a una cantidad real de oro en reserva. Esta inestabilidad lleva a una creciente preocupación en la sociedad sobre la verdadera validez de su dinero.

Este cambio marca un momento crucial en la historia del dinero, donde se pasa de un sistema monetario respaldado por metales preciosos a uno en el que el valor del dinero es establecido por la confianza y no por un bien tangible: la **moneda fiduciaria**.

Esta transición no fue repentina sino que resultó de un proceso gradual. Fue alimentada por eventos históricos significativos como la Revolución Industrial, que trajo consigo la expansión económica y la complejidad en las **transacciones**. Además, el surgimiento de sistemas financieros más sofisticados y la creación de bancos centrales fueron factores clave que contribuyeron a este cambio. Estos avances permitieron la aparición de un sistema financiero más flexible pero también suscitaron nuevas preguntas acerca de la seguridad y la confiabilidad del dinero en este nuevo paradigma.

Se llega a la era de la Primera Guerra Mundial, una época marcada por el tumulto global. Hasta entonces, la convertibilidad del papel moneda en oro ofrecía una forma tangible de seguridad. Sin embargo, las devastaciones de las guerras mundiales y la Gran Depresión de 1929 erradicaron esa certidumbre.

En el año 1944, las principales naciones del mundo firman el Acuerdo de Bretton Woods, estableciendo al dólar estadounidense como la moneda de reserva global. Este sistema vincula el valor del dólar al oro a \$35/oz y, a su vez, las monedas de otros países al dólar, proporcionando cierta estabilidad en un entorno financiero global volátil.

No obstante, la solidez de este sistema comienza a tambalearse hacia el final de la década de 1960. Esta inestabilidad alcanza su punto culminante con el **"Shock de Nixon"** en 1971, cuando los Estados Unidos anuncian la suspensión de la convertibilidad del dólar en oro. Este evento marca el fin del patrón oro y da lugar a una nueva era financiera centrada en la creación y acumulación de deuda.

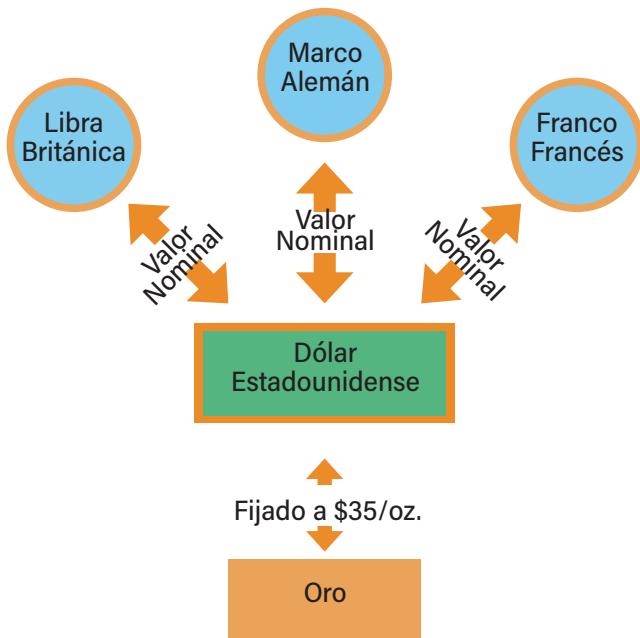
Con esto, la percepción del dinero experimenta un cambio dramático. Lo que antes se consideraba un valor estable y seguro ahora se convierte en algo volátil, sin respaldo físico como el oro. Se vive en una nueva realidad donde el valor del dinero depende de la confianza en un sistema económico que parece estar siempre en flujo, casi como si se estuviera caminando sobre terreno inestable.

**"No creo que tengamos dinero de calidad hasta que no se lo saquemos al gobierno... Lo único que podemos hacer es encontrar una forma inteligente y audaz de introducir algo que no puedan frenar."**

*Friedrich Hayek -Premio Nobel de Economía en 1974*

# Del Trueque al BTC y los CBDC: Un Viaje a Través del Tiempo

## Sistema de Bretton Woods (1945-1972)



A pesar de los esfuerzos por mejorar la calidad de vida, el nivel de bienestar de la mayoría de la gente empieza a disminuir debido a:

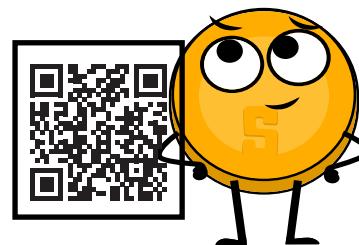
- Abuso de la centralización
- Aumento de los precios
- Estancamiento de los salarios reales
- Debilitamiento de las monedas
- Necesidad de gastar más dinero en menos cosas
- Inestabilidad política
- Deuda, tanto personal como nacional

Estos desafíos pueden ser particularmente difíciles para las personas con menos recursos económicos, lo que puede afectar su capacidad para alcanzar el éxito. Como resultado, la brecha entre los ricos y los pobres parece estar aumentando cada vez más.

Se observan las ramificaciones de este cambio en la economía global, lo que lleva a cuestionamientos sobre la estabilidad y confiabilidad de las monedas fiduciarias. En esta nueva realidad, se comprende que el dólar ya no es una constante fija, sino una moneda susceptible a manipulación y fluctuaciones en su valor.



**LA HISTORIA DE BRETON WOODS EN 3 MINUTOS**  
En medio de un mundo económico turbulento, el dominio del dólar estadounidense como divisa global está siendo sometido a prueba como nunca antes. Pero, ¿qué sucederá cuando el dólar se tambalee y eventualmente ceda su estatus de moneda de reserva?



A medida que el mundo sigue evolucionando y enfrentando desafíos económicos, es fundamental explorar nuevas ideas y soluciones para crear un sistema monetario más justo, estable y sostenible. El futuro del dinero comienza cada vez más a ser un tema de debate y experimentación global.



## Capítulo #2

### 2.4 Trazando la Evolución del Dinero Plástico al Digital

Desde que apareció la primera tarjeta de crédito en los años 50, las cosas han cambiado mucho. Antes, comprar algo era tan fácil como deslizar una tarjeta. Pero eso nos llevó a gastar más de lo que teníamos, haciendo que todo sea más caro en general.

Con el tiempo, Internet cambió cómo usamos el dinero. Ahora podemos hacer casi todo en línea, desde comprar cosas hasta manejar nuestras cuentas bancarias. Esto ha hecho que el efectivo sea menos necesario. Algunos países incluso están pensando en eliminar el efectivo y usar solo monedas digitales.

Pero todo cambió en 2008. La empresa Lehman Brothers quebró, y mucha gente empezó a desconfiar de los bancos y del dinero tal como lo conocíamos. Fue en ese momento de crisis que se creó **bitcoin**, un nuevo tipo de dinero que no necesita bancos y que es más difícil de manipular. Se convirtió en una alternativa para aquellos que ya no confiaban en el sistema financiero tradicional.

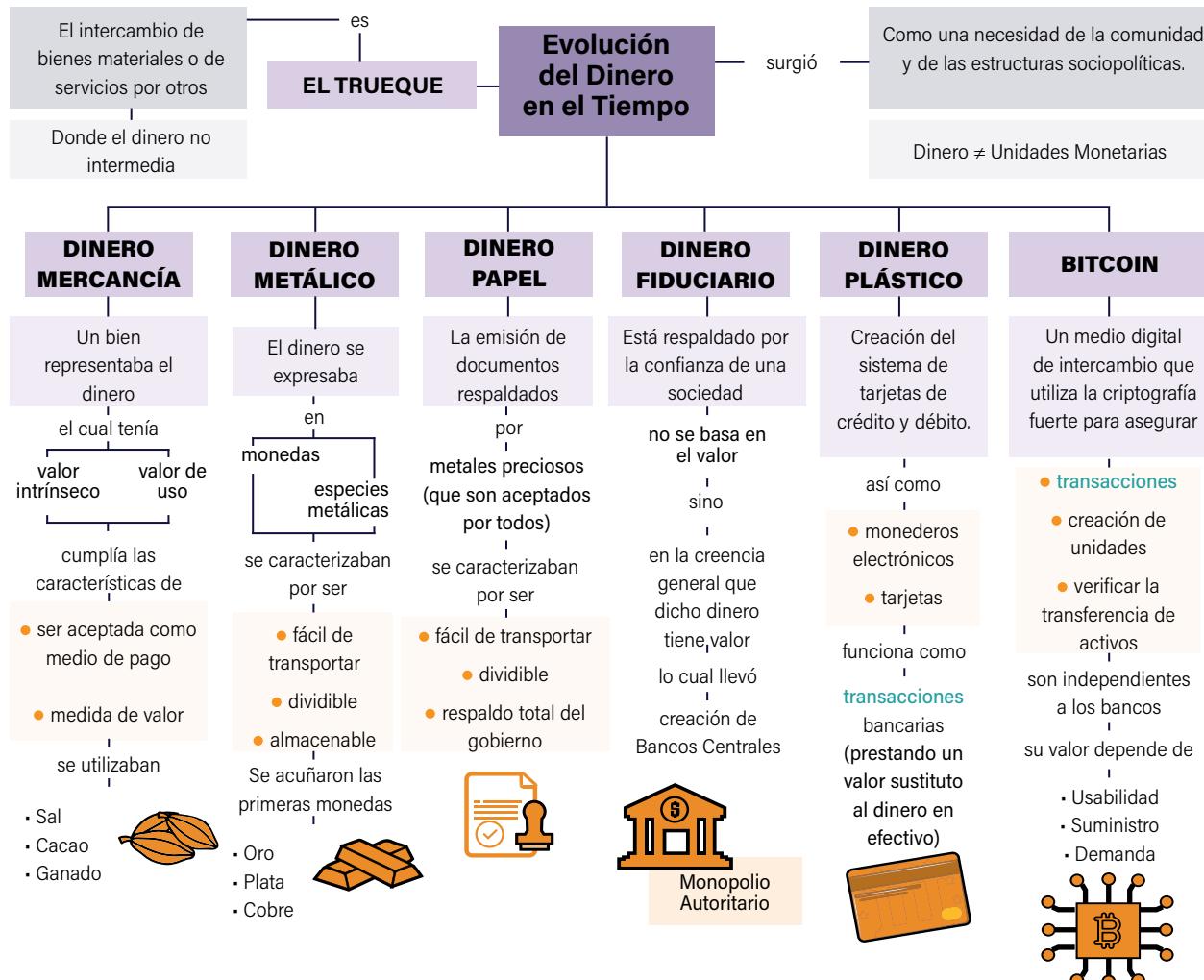
Es verdad que **Bitcoin** tiene desafíos importantes que superar, desde su volatilidad hasta preguntas sobre su seguridad y privacidad. También enfrenta la resistencia de ciertos gobiernos e instituciones financieras que no están dispuestos a reconocerlo como una forma legítima de dinero. A pesar de estos obstáculos, la popularidad de **Bitcoin** sigue en aumento, abriendo nuevas posibilidades para la innovación financiera.

No obstante, su popularidad sigue en aumento, impulsando desarrollos tecnológicos innovadores y abriendo la puerta a explorar nuevos horizontes financieros. De esta forma, la evolución del dinero ha dado un salto cualitativo: desde los **bienes valiosos** de eras antiguas, pasando por el **dinero fiduciario**, hasta llegar a esta nueva era de **dinero digital** y robusto. Por primera vez en casi un siglo, la idea de un dinero respaldado por un valor intrínseco resurge con fuerza. Así, hemos venido a cerrar un círculo: desde una forma de dinero sólido, pasando por períodos de incertidumbre, y retornando a una versión más sólida y digital del concepto de dinero.



# Del Trueque al BTC y los CBDC: Un Viaje a Través del Tiempo

## 2.5 El Dinero y el Tiempo: Un Enlace Inseparable



Iniciar un viaje a través de la historia del dinero es explorar la evolución de los medios que hemos utilizado para representar e intercambiar valor. Desde los tiempos de trueque, pasando por el oro y la plata, hasta las monedas y billetes que conocemos hoy, y finalmente al dinero digital. Cada uno de estos medios de intercambio ha tenido un impacto significativo en la economía y en la sociedad, así como en cómo percibimos y utilizamos nuestro tiempo.





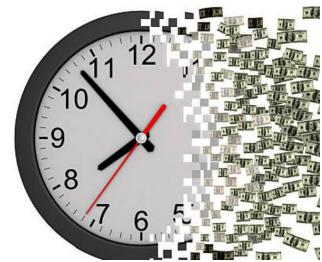
## Capítulo #2

Pero, ¿qué tiene que ver el tiempo con el dinero? La relación entre el tiempo y el dinero es más profunda de lo que podría parecer a primera vista. Podríamos considerar el dinero como una representación de nuestro tiempo. Cuando trabajamos, estamos intercambiando nuestro tiempo, nuestras habilidades y nuestra energía por una compensación monetaria. El dinero, por lo tanto, no es más que la cristalización de nuestro tiempo y esfuerzo.

Este concepto puede parecer abstracto, pero al desglosarlo, observamos cuatro formas distintas en las que el dinero y el tiempo están intrínsecamente vinculados.

- **Tiempo de Trabajo:** Aquí el dinero se convierte en una representación tangible del tiempo que una persona ha dedicado a su trabajo. Cuando intercambias tus horas, tu esfuerzo y tus habilidades por un salario, cada centavo ganado se convierte en un representante de tu tiempo invertido.
- **Tiempo de Consumo:** En esta dimensión, el dinero representa el tiempo necesario para adquirir o consumir bienes y servicios. Por ejemplo, si un artículo cuesta \$10 y tu salario es de \$10 por hora, ese artículo te cuesta una hora de tu tiempo laboral.
- **Tiempo Ahorrado:** El dinero también puede actuar como un medio para ahorrar tiempo. Este ahorro de tiempo ocurre cuando puedes pagar por servicios que te permiten liberar tiempo en tu día. Un ejemplo de esto sería contratar un servicio de limpieza para tu hogar, lo que te ahorra las horas que tendrías que haber dedicado a limpiar.
- **Tiempo Futuro:** Cuando ahorras o inviertes tu dinero, lo estás viendo como 'tiempo futuro'. En esencia, estás reservando parte de tu tiempo laboral actual (en forma de dinero) para usarlo en un momento futuro, como puede ser la jubilación, una compra importante o una situación de emergencia.

El dinero nos hace ponderar entre gratificación inmediata y futura, algo que se ilustra en pruebas como el 'test del marshmallow'. Gastar al instante favorece el presente pero sacrifica el futuro; ahorrar o invertir hace lo opuesto. En un mundo incierto, tener una visión a largo plazo puede ser vital para la estabilidad financiera. Así, el dinero y el tiempo están estrechamente ligados, reflejando cómo cada uno afecta nuestra relación con el otro. A pesar de esta intrincada relación, es crucial recordar que el tiempo, al final del día, es el recurso más valioso que poseemos.





# Capítulo #3



## Descubriendo el Lado Oscuro del Dinero Fiduciario

3.0 Las Mayores Amenazas para tu Dinero: Inflación,  
Devaluación y Pérdida de Poder Adquisitivo

3.1 Desventajas del Sistema Fiat

3.1.1 Los Efectos de la Inflación: Actividad de Subasta

3.1.2 Ahorrar Dinero en Tiempos Difíciles

3.1.3 El Valor Temporal del Dinero y su Importancia  
en el Crecimiento Económico

3.2 El papel del Banco Central en el Manejo del Dinero

3.3 La Magia de la Creación de Dinero

3.3.1 La Banca de Reserva Fraccionaria

3.3.2 Actividad. Banca con Reserva Fraccionaria

3.4 Deuda: La Carga que Aplasta a las Clases Media y Baja

3.4.1 La Toma de Decisiones



# Descubriendo el Lado Oscuro del Dinero Fiduciario

## 3.0 Las Mayores Amenazas para tu Dinero: la Inflación, la Devaluación y la Pérdida de Poder Adquisitivo

En este capítulo, analizaremos el sistema monetario fiduciario, un modelo que a pesar de ser prevalente, esconde considerables desafíos.

Esencialmente, el dinero fiduciario es una moneda sin soporte en bienes tangibles como el oro o la plata. Son puras hojas de papel cuyo valor es universalmente aceptado debido a un decreto gubernamental. Sin embargo, radica aquí su vulnerabilidad fundamental: el gobierno tiene el poder de emitir tanto papel como desee, situación que puede precipitar inflación y devaluación de la moneda. ¿Quiénes son los más perjudicados en este escenario? Sin duda, la población ordinaria, como tú y yo.



La **inflación** ocurre cuando el nivel general de precios de los bienes y servicios en una economía aumenta con el tiempo. Refleja una disminución del **poder adquisitivo** del dinero y provoca una pérdida de valor real del medio de cambio y la unidad de medida dentro de una economía.

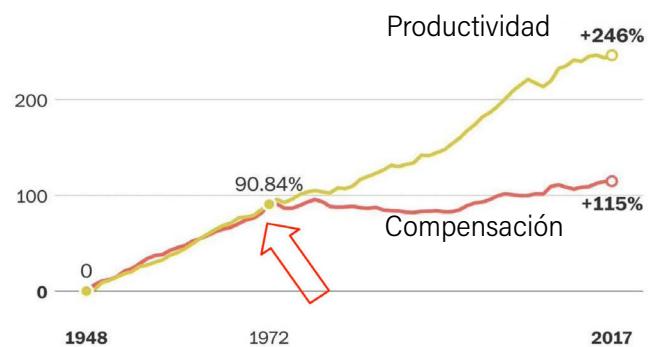


El **poder adquisitivo** se refiere a la cantidad de bienes o servicios que se pueden comprar con una cantidad determinada de dinero. En otras palabras, es una medida de cuánto puedes comprar con tu dinero.



Además, la **devaluación** de la moneda ocurre cuando el gobierno reduce el valor de su moneda al aumentar la **oferta monetaria** o disminuir la calidad de la moneda.

Crecimiento en Productividad y Compensación por Hora (1948-2017)



NOTA: La compensación incluye salarios y beneficios para trabajadores de producción y no supervisores.



¿Habrá recesión en el 2023?



- Por ejemplo, si tienes \$100 y el precio de un pan es de \$2, puedes comprar 50 panes con tu dinero. Sin embargo, si se produce inflación y el precio del pan aumenta a \$4, tu poder adquisitivo disminuye y solo puedes comprar 25 panes con tus \$100.





## Capítulo #3



### Oferta Monetaria:

Es el **total** de dinero en circulación en cualquier economía en un momento dado, incluyendo la moneda física y el dinero digital en las cuentas bancarias. La oferta monetaria es fundamental en economía, ya que puede influir en la salud general de la misma.

### Inflación y Folletos de Oferta 2007 vs 2023: Aumentos de hasta 41700%



En un mundo donde la tecnología avanza rápidamente, uno esperaría que la calidad de vida mejorara y los precios de los bienes y servicios disminuyeran. Sin embargo, en la realidad, enfrentamos una creciente desigualdad de ingresos y pérdida de poder adquisitivo, especialmente para las clases media y baja. De hecho, según el Índice de Desigualdad Global 2020 del World Inequality Lab, el 10% más rico controla el 52% del ingreso mundial, mientras que el 50% más pobre solo recibe alrededor del 8.5%.

Esta desigualdad se agrava aún más por factores como la inflación y la devaluación, que erosionan el poder adquisitivo de los más vulnerables. Esto se vio claramente en crisis como la financiera de 2008 y la pandemia de COVID-19, donde las medidas de alivio beneficiaron principalmente a las grandes corporaciones y a los más ricos, dejando a la mayoría luchando por sobrevivir.

Por otro lado, se nos ha hecho creer que una inflación moderada es necesaria para el crecimiento económico, pero en realidad, actúa como un impuesto oculto que afecta desproporcionadamente a los menos acaudalados. Además, el sistema financiero actual, controlado por bancos centrales y gobiernos, tiene el potencial de exacerbar estos problemas. Puede ajustar las políticas y tasas de interés para beneficiar a ciertos grupos mientras pone en desventaja a otros, todo mientras acumula deudas enormes que las futuras generaciones tendrán que pagar.

Frente a estos retos, surgen alternativas como **Bitcoin**, que ofrecen un sistema financiero más transparente y posiblemente más justo. Es hora de cuestionar y reformar nuestro sistema financiero para que sea más equitativo y sostenible para todos.

Fuente: Focus Market

Entonces, ¿qué es la inflación?  
¿Por qué es tan peligrosa? Este  
vídeo resuelve estas preguntas.



# Descubriendo el Lado Oscuro del Dinero Fiduciario

## 3.1 Desventajas del Sistema Fiat

### 3.1.1 Los Efectos de la Inflación: Una Actividad de Subasta

**Objetivo:** Entender el concepto de oferta monetaria y su impacto en los precios de los productos y servicios en una economía.



**Subasta:** Venta pública donde bienes o propiedades se venden al postor que ofrezca el mayor precio.

Participarás en tres rondas de subasta donde se subastarán barras de chocolate idénticas en cada ronda

1. Tu profesor comenzará la actividad distribuyendo una cantidad aleatoria de dinero de monopolio a cada estudiante. Esto representará la oferta monetaria de una sociedad. Asegúrate de recordar cuánto dinero has recibido al principio.

2. Posteriormente, se pondrá a subasta una barra de chocolate. Podrás hacer ofertas usando tu dinero de monopolio, y la oferta más alta se llevará la barra de chocolate. Presta atención a cuánto dinero se utiliza en esta oferta ganadora.

3. A continuación, tu profesor añadirá una cantidad significativa de dinero de monopolio a la oferta monetaria total, representando un aumento de la oferta monetaria por parte del gobierno. Este dinero adicional se distribuirá solo entre algunos estudiantes elegidos al azar, representando el efecto Cantillon. Observa cómo esto afecta a la distribución de la riqueza en tu clase.

4. Luego, se realizará una segunda subasta de una barra de chocolate idéntica. Toma nota de cómo la oferta monetaria adicional afecta las ofertas y los precios.

5. Para la tercera ronda, en lugar de añadir más dinero a la oferta monetaria, se reducirá el premio disponible. Por ejemplo, se subastará solo media barra de chocolate, o un premio más pequeño. Esto representa la escasez de recursos naturales.

6. En la última subasta, observa cómo la menor cantidad de bienes disponible afecta las ofertas y los precios.



## Capítulo #3

Ronda	Oferta Monetaria	Oferta Ganadora

Al final de la actividad, reflexiona sobre cómo la oferta monetaria, la distribución de la riqueza y la escasez de recursos pueden afectar los precios y el comportamiento económico.

1. ¿Cuál fue la oferta monetaria total de la clase en cada ronda de la subasta?
2. ¿Cómo cambiaron las ofertas y los precios con el aumento de la oferta monetaria?
3. ¿Cómo afectó la distribución desigual del dinero a los precios y las ofertas?
4. ¿Cómo cambió la situación cuando se redujo la cantidad de bienes disponibles?
5. ¿Cómo se reflejaron en la actividad los conceptos de inflación, efecto Cantillon y escasez de recursos? (Contestaremos esta pregunta al acabar la sección 3.3)
6. ¿Cómo se pueden aplicar estos conceptos a situaciones de la vida real y qué implicaciones tienen para la economía en su conjunto?

Comprender las repercusiones de la inflación, tanto a nivel personal como colectivo, capacita a las personas para tomar decisiones de ahorro y gasto más informadas, al tiempo que destaca los obstáculos que el panorama económico actual impone. Comenzaremos con un ejemplo ilustrativo.

Conozcan a Jaime, un estudiante universitario que reside en un pequeño apartamento y tiene un empleo de medio tiempo en una cafetería para cubrir sus gastos diarios y los costos universitarios. Desde que comenzó su vida independiente, Jaime se ha convertido en un experto en la administración de sus finanzas, llevando un registro meticuloso de sus **ingresos** y **gastos** a través de un libro de cuentas.



Un **libro de cuentas** es un registro detallado de todas tus **transacciones** monetarias, tanto **ingresos** como **gastos**. Te ayuda a mantener el control de tus finanzas personales.

Al inicio del año, Jaime presupuestó \$10,000 para sus gastos de manutención, incluyendo alquiler, comida y otras necesidades.

# Descubriendo el Lado Oscuro del Dinero Fiduciario

Aquí están sus **transacciones** de enero:

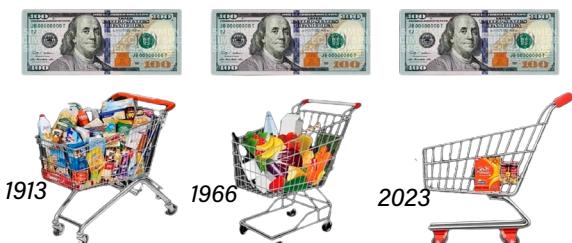
Fechas	Descripción	Facturas	Tipo	Balance
01/01/2023	Saldo Inicial			\$1,600.00
01/01/2023	Alquiler de Enero	\$800.00	Débito	\$800.00
01/05/2023	Comestibles	\$100.00	Débito	\$700.00
01/15/2023	Cheque de Medio Tiempo	\$500.00	Crédito	\$1,200.00
01/20/2023	Gasolina para el Auto	\$350.00	Débito	\$850.00
01/30/2023	Libros de Texto	\$200.00	Débito	\$650.00

Este libro muestra que el saldo inicial en la cuenta de Jaime el 1 de enero era de \$1,600, de los cuales **gastó** \$800 para pagar el alquiler del mes. Luego, **gastó** \$100 en comestibles (un **débito**) y **recibió** \$500 (un **crédito**) de su trabajo, aumentando su saldo a \$1,200. Después, **gastó** dinero en gasolina y libros de texto, dejando su saldo en \$650 al final del mes.

Un año después, mientras almuerza con su abuelo, Jaime se da cuenta de que su presupuesto ya no es suficiente debido al aumento de los precios de los bienes y servicios que necesita. Entonces, ve una imagen que muestra el cambio en los precios de los ingredientes de una hamburguesa en sólo un año y se queda sin palabras.

Cuando lo comenta con su abuelo, este le cuenta cómo, en 1956, ganaba \$100 al mes trabajando en una fábrica, lo que en aquel entonces era un sueldo decente. Con ese salario, pudo ahorrar lo suficiente para comprar una casa en las afueras de la ciudad.

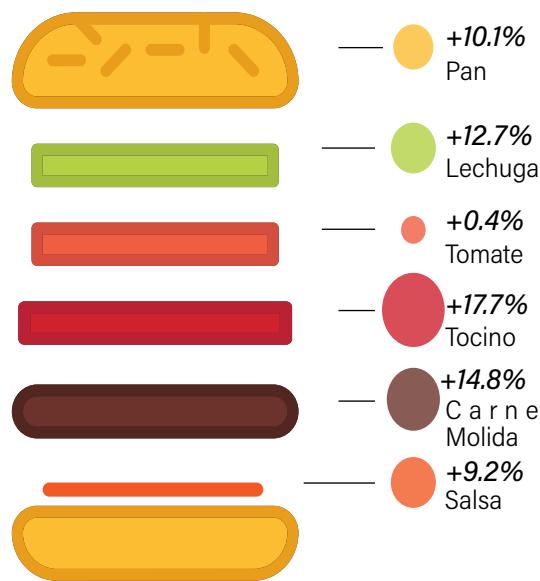
La capacidad de Jaime para comprar bienes y servicios ha sufrido un descenso notable, evidenciado por el incremento de precios de los productos en su "canasta" habitual. A través de su registro contable, Jaime nota una reducción en su poder adquisitivo a lo largo del año, lo que le impulsa a realizar ajustes en su presupuesto.



Para entender la magnitud de este impacto, es útil ponerlo en contexto. Por ejemplo, en 1913, se podían comprar 30 tabletas de chocolate Hershey's por solo \$1, mientras que en 2020, esa misma cantidad costaría \$26.14. Esta comparación resalta cómo ha cambiado el valor de la moneda a lo largo del tiempo debido a la inflación.

## Cómo la Inflación Cambió el Precio de una Hamburguesa

Variación interanual del precio de ingredientes seleccionados de una hamburguesa (2021 – 2022)

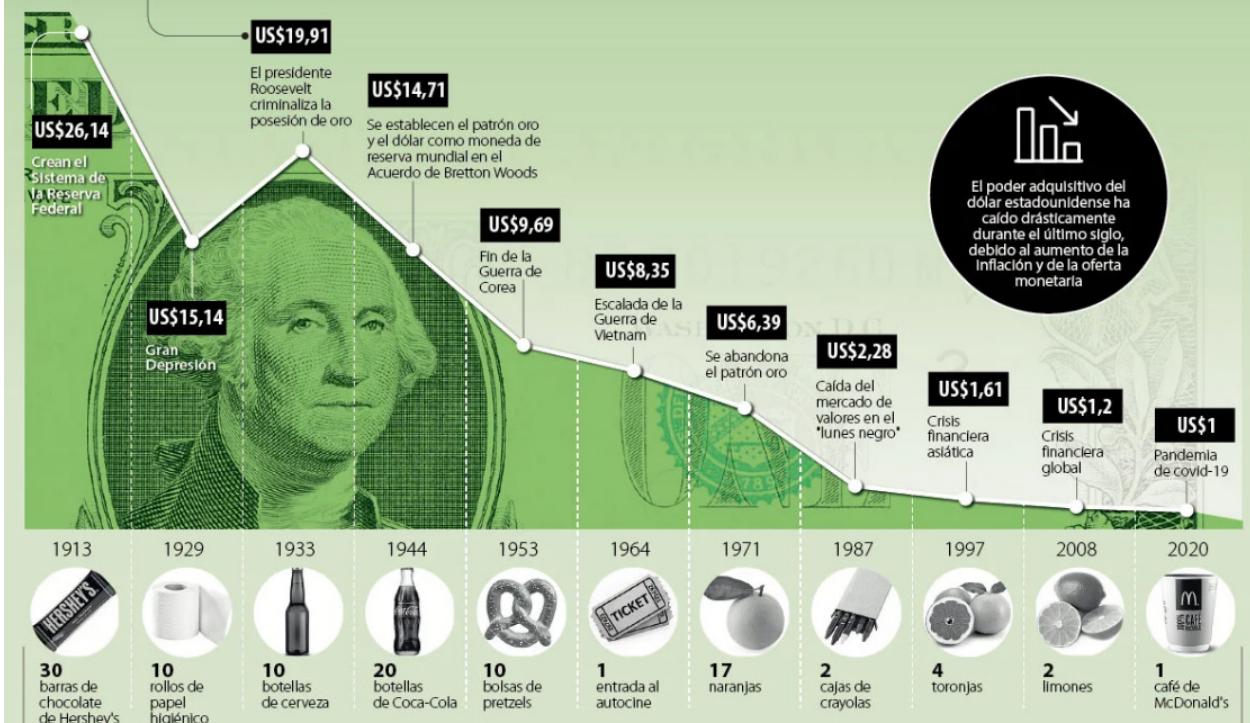




## Capítulo #3

### LA CAÍDA DEL PODER ADQUISITIVO DEL DÓLAR EN EL ÚLTIMO SIGLO

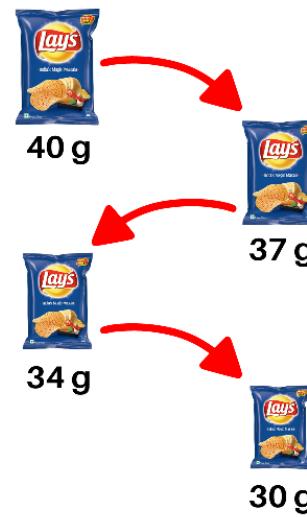
Poder adquisitivo de US\$1



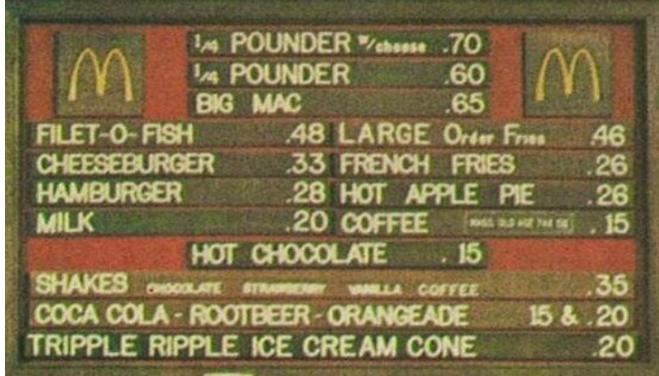
LO QUE COMPRABAS ESE AÑO CON \$1 USD EN ESE AÑO

Según datos de la Oficina de Estadísticas Laborales de Estados Unidos, los precios actuales son más de 30 veces mayores que en 1913. En términos simples, lo que hoy compras con un dólar, en 1913 lo comprabas con aproximadamente 3 centavos. Si Jaime pudiera viajar en el tiempo y llevar \$100 a 1913, en términos de poder adquisitivo, sería como tener solo \$3 en 2023.

Aunque Jaime tiene un salario más alto que el de su abuelo, la inflación constantemente reduce el valor real de su dinero, lo que desalienta el ahorro y complica la planificación financiera a largo plazo. Para empeorar la situación, enfrenta otra forma de erosión de su poder adquisitivo, conocida como inflación encubierta. En este fenómeno, el precio de los productos y servicios se mantiene aparentemente constante, pero la cantidad o calidad de lo que se compra disminuye. Por ejemplo, podría notar que las papitas tienen la misma etiqueta de precio pero viene con menos contenido o menor calidad.



# Descubriendo el Lado Oscuro del Dinero Fiduciario



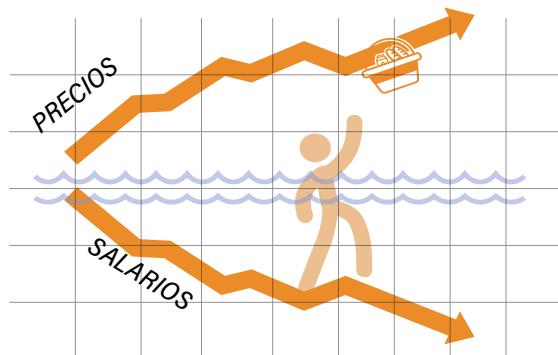
McDonald en 1970

## McMENÚ DEL DÍA



McDonald en 2020

Un ejemplo claro de esto es la industria de la comida rápida, donde podemos ver cómo la hamburguesa Big Mac de McDonald's ha disminuido en tamaño con el tiempo, aunque su precio ha permanecido igual. De manera similar, en el caso de los productos electrónicos, la obsolescencia programada hace que los dispositivos sean menos duraderos en comparación con décadas anteriores. Estas prácticas disminuyen aún más el poder adquisitivo de las personas y complican la posibilidad de mantener un nivel de vida sostenible a largo plazo.



Cuando paramos a pensar en los costos crecientes de la vida, como el precio de la gasolina o el alquiler de vivienda, resulta evidente que nuestros salarios no se estiran como antes. La inflación ha estado avanzando a un ritmo más rápido que los aumentos salariales, lo que nos pone en una situación complicada para mantener un estilo de vida que creímos sostenible.

Para ajustarse a la inflación y preservar su poder adquisitivo, Jaime necesita incorporar \$1,000 adicionales a su presupuesto si desea mantener el estilo de vida que llevaba el año anterior. Esto implica que su capacidad de compra ha disminuido en \$1,000, dado que ahora necesita invertir una mayor cantidad de dinero si no quiere sacrificar sus gustos o necesidades. La siguiente tabla muestra el costo de cada artículo de la cesta en el primer y segundo año, así como el aumento porcentual del precio:

Artículo	Costo Año #1	Costo Año #2	Aumento %
Alquiler	\$4,000	\$4,500	12.5%
Comestibles	\$2,000	\$2,300	15%
Necesidades	\$4,000	\$4,200	5%
<i>Total</i>	<i>\$10,000</i>	<i>\$11,000</i>	<i>10%</i>



# Capítulo #3

## Nuestra Realidad:

En el panorama económico de 2023, nos encontramos frente a una realidad preocupante: una tasa de inflación global que excede el 7% anual y una amenaza creciente de recesión mundial. Estas condiciones han desencadenado una serie de desafíos que afectan a individuos, empresas y gobiernos en formas variadas:

### 1. Inflación e Impacto Distributivo:

La inflación redistribuye riqueza entre distintos grupos, golpeando especialmente a los más pobres. Como estos destinan una gran parte de su ingreso a alimentos, cuyo precio suele subir más rápido, se ven más afectados por la inflación.

#### Los pobres, los más perjudicados

Los mayores precios de los alimentos y la energía provocados por la inflación afectan sobre todo a los más pobres.  
(variación porcentual interanual)



### 2. Erosión de los ahorros e inversiones:

La inflación alta devalúa ahorros e inversiones. Un fondo de jubilación de \$500,000, por ejemplo, pierde poder adquisitivo pues esa cantidad ya no compra lo mismo que antes.

### 3. Deudas complicadas:

La inflación influye en las deudas de forma diversa. Una hipoteca fija se vuelve menos pesada, ya que disminuye el valor real de pagos futuros. Pero las tarjetas de crédito con tasas variables pueden ver aumentar los intereses a pagar si la inflación sube.

### 4. Desafíos para las empresas:

Imagina tener una pequeña panadería y que, con la inflación alta, los costos de harina, azúcar y electricidad suben. Debes decidir si aumentar los precios de tus productos, recortar gastos o buscar mejorar la eficiencia.

### 5. Cambios en la política gubernamental:

Para controlar la inflación, el gobierno puede subir las tasas de interés o reducir el gasto público. Esto puede afectar tus planes de compra de casa o financiación de negocios, pues los préstamos son más caros con las altas tasas de interés del Banco Central.

Estos ejemplos ilustran cómo una alta inflación puede impactar distintos aspectos de la economía y la vida cotidiana. Aunque no te han quitado dinero directamente como en un impuesto tradicional, el poder de compra de tu dinero ha disminuido. Es como si te hubieran "cobrado" algo sin que te des cuenta. Eso es lo que se suele llamar un "impuesto oculto" cuando se habla de inflación. Pierdes capacidad de comprar cosas, incluso si la cantidad de dinero que tienes se queda igual. En tiempos como estos, es vital contar con una administración financiera sólida y una estrategia económica bien fundamentada.



# Descubriendo el Lado Oscuro del Dinero Fiduciario

## 3.1.2 Ahorrar Dinero en Tiempos Difíciles

Nos encontramos en una etapa crucial, con la economía mundial azotada por la persistente inflación, el rápido aumento de las tasas de interés y una creciente incertidumbre sobre una posible recesión global. Este entorno hace que el ahorro sea un desafío, ya que la inflación erosiona el valor de nuestro dinero y las crecientes tasas de interés pueden generar deudas más costosas.

Aunque la situación puede parecer desalentadora, es importante recordar que existen estrategias para salvaguardar tus finanzas y asegurar la estabilidad financiera. Aquí te presentamos algunas ideas para enfrentar estos desafíos:

### Presupuesto detallado:

¿Conoces el plan de ahorro del método **50/30/20?**



**Necesidades (50%):** Gastos esenciales como vivienda, comida, transporte y atención médica.

**Quieres (30%):** Gastos discrecionales para cosas que aumentan tu calidad de vida pero no son esenciales.

**Ahorros e Inversiones (20%):** Dinero destinado a ahorros, inversiones y liquidación de deudas.

#### Elabora un presupuesto preciso para administrar mejor tus finanzas:

Realiza un seguimiento exhaustivo de tus gastos para identificar oportunidades de reservas.

#### Objetivos de ahorro y diversificación de inversiones:

Ante un escenario de tasas de interés en alza, revisa tus opciones de inversión. La diversificación es clave para minimizar riesgos. Cada opción tiene su propio conjunto de ventajas y desafíos, lo que permite un equilibrio en tu cartera de inversión.

#### Fondo de emergencia sólido:

Reserva un fondo de emergencia para cubrir entre 6 y 12 meses de gastos. Te servirá de respaldo ante desempleo u otras dificultades financieras.

#### Minimización de gastos y consumo consciente:

Evita gastos superfluos y adopta un enfoque consciente de consumo. Aprovecha descuentos y evita compras impulsivas.

#### Reutilizar, reparar y reciclar:

En vez de comprar nuevos artículos, considera reparar, actualizar o reutilizar lo que ya tienes. El trabajo manual puede resultar en ahorros significativos.

En momentos de inestabilidad financiera, cada ahorro cuenta y puede tener un impacto a largo plazo. Al controlar tus finanzas y adaptarte a la economía fluctuante, te preparas mejor para enfrentar futuros desafíos económicos.



## Capítulo #3

### 3.1.3 El Valor Temporal del Dinero y su Importancia en el Crecimiento Económico

¿Alguna vez te has preguntado por qué los bancos ofrecen tantos servicios? A pesar de que parezca que son generosos, debes recordar que los bancos son negocios cuyo principal objetivo es obtener ganancias. Pero, ¿cómo generan ganancias si lo que hacen es prestar dinero?



Al prestar dinero a tasas de interés más altas de las que lo reciben, los bancos pueden obtener *ganancias*. También generan ingresos mediante comisiones y actividades de inversión.

Pero, ¿por qué es relevante este concepto para ti como individuo? Probablemente hayas escuchado la frase "un dólar hoy vale más que un dólar mañana". Introducimos el concepto del **valor temporal del dinero**, el cual señala que el dinero tiene más valor en el presente que en el futuro. Las razones principales son las oportunidades de inversión que permiten generar rendimientos y la pérdida de valor del dinero a lo largo del tiempo debido a la inflación.

Endeudarse puede ser aceptable siempre y cuando el dinero se utilice para generar ingresos y aumentar el poder adquisitivo en el futuro. Pedir dinero prestado puede permitir a individuos o empresas realizar inversiones que incrementen su productividad y eficiencia, lo cual se traduce en mayores beneficios y estabilidad financiera.

Por ejemplo, si un agricultor solicita un préstamo para adquirir equipos nuevos que le permitan cosechar de manera más rápida y eficiente, podrá generar mayores ingresos y aumentar su poder adquisitivo. En cambio, si el dinero se malgasta o se invierte en proyectos improductivos, esto podría generar dificultades financieras y no sería una decisión acertada.



*El propósito de invertir es lograr un rendimiento que supere la tasa de inflación*, permitiendo que tu dinero preserve su poder adquisitivo a lo largo del tiempo. De esta manera, el valor de tu dinero en el futuro podría ser mayor que su valor actual.

Si almacenas tu dinero en una cuenta de ahorros con una tasa de interés baja, su poder adquisitivo en el futuro disminuirá. Sin embargo, si inviertes en opciones con posibles rendimientos más elevados, estarás mejor preparado para enfrentar una economía difícil y salir adelante.



Los bancos piden dinero prestado a un interés bajo (digamos 5%)



Los bancos prestan este dinero a los prestatarios a una tasa de interés más alta (digamos 9%)



Los bancos pagan intereses de los intereses recibidos por los préstamos ( $9\% - 5\% = 4\%$ ) y se quedan con el resto como su ganancia

# Descubriendo el Lado Oscuro del Dinero Fiduciario

## 3.2 El Papel del Banco Central en el Manejo del Dinero

Para entender cómo funciona el dinero en nuestra sociedad, debemos conocer cómo los bancos centrales y los gobiernos manejan el suministro de dinero. Estudiar estos temas nos ayuda a entender por qué **bitcoin**, una moneda digital que no controla ningún gobierno, se creó. En esta sección, explicaremos cómo los bancos centrales tienen un papel crucial en la forma en que se maneja el dinero en nuestra economía.



El **Banco Central** maneja la oferta monetaria del país y actúa como banquero de los bancos comerciales, controlando la cantidad de dinero en circulación con el fin de mantener la inflación a un nivel deseado y maximizar el empleo. Por ejemplo, en Estados Unidos, este papel recae en la Reserva Federal (Fed).

Las políticas que los gobiernos y los bancos centrales implementan para gestionar la economía son las políticas **monetarias y fiscales**. Aunque ambas políticas están destinadas a influir en la economía, difieren en sus enfoques, objetivos y responsables.

### La Política Monetaria y la Política Fiscal

La política monetaria se ocupa de controlar la oferta de dinero, la inflación y las tasas de interés, con el fin de influir en el crecimiento económico y el empleo.

Esta política es implementada por los bancos centrales, que utilizan diversas herramientas, como la modificación de las tasas de interés, la compra y venta de **bonos del gobierno** y la regulación de los requerimientos de reservas bancarias.

Imaginemos que la inflación está aumentando rápidamente, lo que significa que los precios de los bienes y servicios están subiendo. Para frenar este crecimiento, el Banco Central puede aumentar las tasas de interés. Cuando las tasas de interés son más altas, la gente tiende a pedir menos préstamos porque cuesta más devolver ese dinero. Esto reduce la cantidad de dinero que circula en la economía, lo que a su vez puede ayudar a bajar la inflación.



Ahora, piensa en cómo podría afectar esto a Jaime, el personaje que mencionamos antes. Si estaba pensando en pedir un préstamo para abrir su propio negocio, ahora podría ser más difícil para él hacerlo porque los intereses son más altos. O si ya tiene un préstamo con una tasa de interés variable, ahora tiene que pagar más cada mes.



## Capítulo #3

Por otro lado, la política fiscal tiene como objetivo influir en la economía mediante el **gasto público y la recaudación de impuestos**, buscando mejorar la distribución de la riqueza, el crecimiento económico y el empleo. Esta política es implementada por el gobierno a través de sus ministerios o departamentos correspondientes, que utilizan el gasto público (inversiones en infraestructura, educación, defensa, etc.) y la política impositiva (tasas de impuestos, exenciones fiscales, deducciones) como herramientas principales.

Supongamos que el gobierno, en un intento de estimular la economía durante un período de inflación alta, decide implementar una política fiscal expansiva. Esto podría implicar una disminución de las tasas impositivas (tributarias) y un incremento en el gasto público.

Jaime, que ha estado lidiando con el impacto de la inflación en su poder adquisitivo, podría verse beneficiado de estas medidas. Con una tasa tributaria más baja, su salario neto podría aumentar, dándole un poco más de dinero para cubrir sus necesidades y las de su familia, a pesar de la inflación.

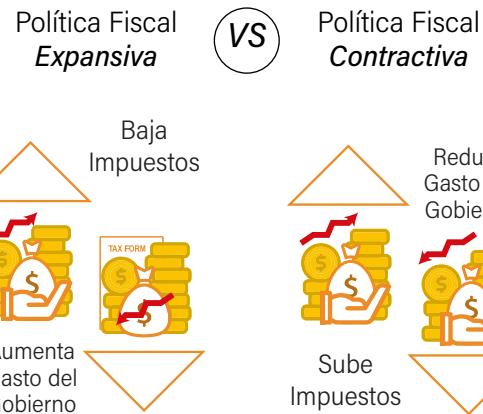
Por otro lado, el incremento del gasto público podría llevar a la creación de empleos o a mejoras en servicios públicos que Jaime utiliza, como transporte o atención sanitaria. Sin embargo, estas medidas también podrían acelerar la inflación si el aumento del gasto público no es compensado con un incremento de la producción en la economía, agravando la erosión del poder adquisitivo de Jaime a largo plazo.

### Relación entre Política Monetaria y Política Fiscal:

La **política monetaria y fiscal**, gestionada respectivamente por el banco central y el gobierno, trabajan conjuntamente para estabilizar y fomentar el crecimiento económico. Por ejemplo, en una recesión, el gobierno puede implementar recortes de impuestos y aumentar el gasto público, mientras que el banco central puede disminuir las tasas de interés para estimular la economía. Es esencial una coordinación efectiva entre estas políticas para garantizar una economía estable y en crecimiento.

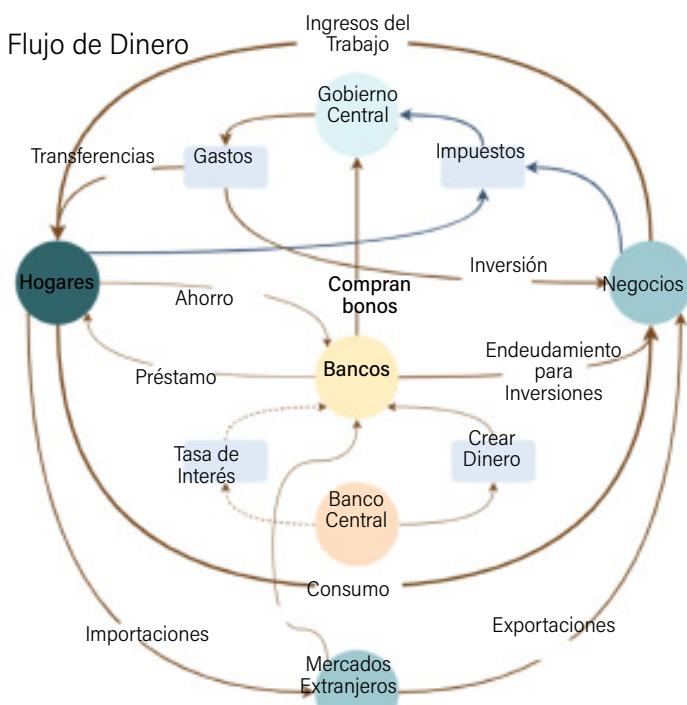
El término "**demasiado grande para caer**" se refiere a instituciones financieras cuyo colapso tendría efectos devastadores en el sistema financiero en general. Un caso reciente es el del Silicon Valley Bank (SVB), que colapsó el 10 de marzo de 2023 tras una retirada masiva de depósitos. Este incidente supuso la tercera mayor quiebra bancaria en la historia de los Estados Unidos.

El colapso del SVB se debió a un incremento en sus tenencias de valores a largo plazo y a pérdidas significativas a causa del aumento de las tasas de interés. A pesar de vender miles de millones en valores y solicitar préstamos extensos, SVB no pudo satisfacer la retirada de \$42 mil millones de sus clientes. Como resultado, el Departamento de Protección Financiera e Innovación de California se hizo cargo del banco y lo colocó bajo la administración de la Corporación Federal de Seguro de Depósitos (FDIC).



# Descubriendo el Lado Oscuro del Dinero Fiduciario

## 3.3 La Magia de la Creación de Dinero



### 3.3.1 La Banca de Reserva Fraccionaria

La ventaja es que ahora el banco tiene la capacidad de utilizar esos fondos adicionales en distintas operaciones financieras. Por ejemplo, puede conceder préstamos a personas que desean comprar una vivienda o a empresas que necesitan invertir en equipo o maquinaria. De este modo, el nuevo capital circula de manera gradual en el sistema financiero, impulsando así la actividad comercial y de inversión.

Vivimos en un sistema bancario donde las entidades financieras solo tienen que retener una parte de los depósitos de sus clientes y pueden prestar el resto. Este modelo, que ha sido la norma desde el siglo XVII, se conoce como **"banca de reserva fraccionaria"**. En él, los bancos solo necesitan mantener una fracción de sus depósitos totales como reserva, y el sobrante puede ser otorgado en préstamos a otros clientes. Al hacer esto, los bancos efectivamente generan más dinero para la economía. Esto sucede porque el dinero prestado eventualmente regresa al sistema bancario en forma de nuevos depósitos, aumentando la cantidad que los bancos pueden volver a prestar.

Imagina que una persona toma un préstamo de \$10,000 del banco para renovar su casa. Ahora tiene \$10,000 adicionales en su cuenta bancaria que no estaban allí antes. Este dinero "nuevo" se gasta en comprar materiales y pagar a los trabajadores.

Imagina que el banco central de un país, digamos la Reserva Federal en Estados Unidos, quiere poner más dinero en la economía. ¿Por qué? Tal vez para ayudar a que las empresas crezcan más rápido o para controlar los precios de las cosas que compramos.

Para hacerlo, el banco central crea \$100 millones de dólares "de la nada" en una computadora. Luego, le da ese dinero a un banco común a cambio de algo que se llama **"bono gubernamental"**, que es como un papel que dice **"te pagaré más tarde"**.

Ahora, el banco común tiene \$100 millones adicionales en su "caja". Pero ese dinero no es un regalo; en el futuro, el banco tiene que devolverlo al banco central, con un poco más por el interés.

### La Crisis del 2008





## Capítulo #3

Digamos que los trabajadores y las tiendas donde compró los materiales depositan ese dinero en sus propios bancos. Ahora esos bancos tienen más dinero en sus "cajas", lo que les permite hacer más préstamos a otras personas y empresas. Por ejemplo, uno de los trabajadores que recibió \$1,000 podría querer comprar una moto. Va al banco y pide un préstamo para hacerlo. El banco le da el préstamo, y él compra la moto. La persona que vendió la moto pone el dinero en su banco, y así continúa el ciclo.

De esta forma, el dinero original de \$100 millones creado por el banco central puede terminar siendo mucho más que eso en la economía real, gracias a este "efecto dominó" de préstamos y depósitos.

Pronto entenderemos que aunque la capacidad de la Fed para inyectar nuevo dinero en la economía ayuda a estimular el crecimiento y alcanzar sus objetivos, este proceso puede tener efectos inesperados, como aumentar la desigualdad de riqueza en la sociedad.



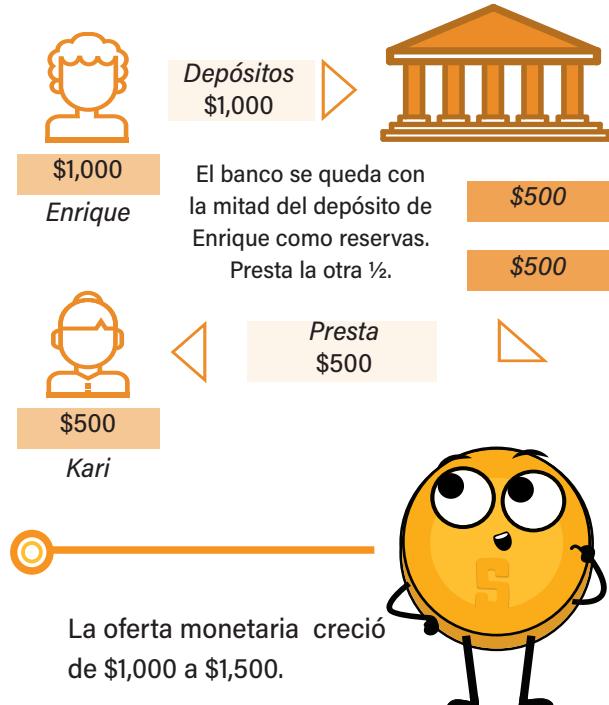
El **efecto Cantillon** explica que la creación de dinero nuevo beneficia principalmente a los primeros receptores, como grandes empresas y personas adineradas, permitiéndoles acumular más riqueza. Por otro lado, las personas con menos recursos enfrentan los efectos negativos de la inflación sin recibir provecho directo del dinero recién creado.

Supongamos que tenemos un banco y cuatro personas: Enrique, Kari, Nicolle y Adam. Este banco debe seguir una regla (llamada fracción de reserva) que dice que solo necesita guardar el 50% de los depósitos de sus clientes y puede prestar el 50% restante.

- Enrique deposita \$1000 en el banco. Siguiendo la regla del 50%, el banco guarda \$500 y le presta \$500 Kari.
- Kari usa esos \$500 para pagarle a Nicolle por un trabajo de traducción, quien luego deposita esos \$500 en el banco.
- Ahora, el banco guarda los \$250 de Nicolle (el 50% de \$500) y presta los otros \$250 a Adam.

Este proceso se repite con las demás personas. El banco originalmente solo tenía \$1000 en efectivo, pero después de este ciclo, efectivamente tiene depósitos por \$2000. Esto no significa que el banco ha creado \$1000 en crédito. En otras palabras, no se ha duplicado el dinero físico, sino que se ha expandido el crédito a través de préstamos.

### Banca de Reserva Fraccionaria Manteniendo ½



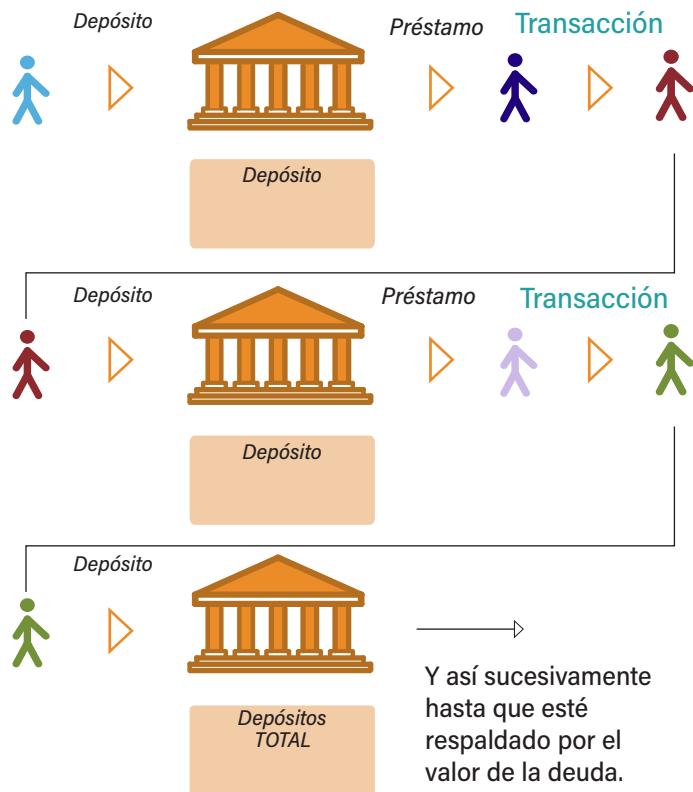
# Descubriendo el Lado Oscuro del Dinero Fiduciario

## 3.3.2 Actividad: Banca con Reserva Fraccionaria

Pero este sistema tiene riesgos. Si no se gestiona adecuadamente, puede llevar a endeudamientos excesivos, inflación y disminución del poder adquisitivo. Es por eso que los bancos centrales ajustan el coeficiente de reserva según las condiciones económicas para tratar de mantener la estabilidad.

Necesitamos los siguientes voluntarios:

- A = Depositante(Ganador de la Lotería) ●
- B = Cajero del Banco ○
- C = Deudor #1 ●
- D = Propietario/Depositante ●
- E = Deudor #2
- F = Propietario de Galería de Arte ○



Ahora inténtalo tu pero asumiendo un coeficiente de reservas del 10%:

Completar todos los campos en blanco:

1. A acaba de ganar \$100.000 dólares en la lotería y los deposita en el banco (B). Con un coeficiente de reservas del 10%, B debe guardar \$  en su caja fuerte y puede prestar los \$  restantes.
2. C pide prestada a B la cantidad máxima \$  y la utiliza para comprar una casa a D.
3. D deposita los \$  recibidos de C en el banco (B). El total de depósitos en el banco es ahora de \$ .
4. E solicita un préstamo a B, y el banco presta el 90% del nuevo depósito, que asciende a \$ .
5. E utiliza el préstamo de \$  para comprar una obra de arte a F, que a su vez deposita el dinero en el banco (B). El total de depósitos registrados es ahora de \$ .

En este escenario, el depósito inicial de \$100.000 dólares ha dado lugar a un total de \$  dólares en depósitos después de circular por la economía.



## Capítulo #3



Has pensado alguna vez en qué cantidad de dinero deberían los bancos guardar en reserva? Imagina cómo cambiaría la economía si esa tasa de reserva se redujera al 5%, al 1%, o incluso llegara a ser cero. Podrías usar el **multiplicador monetario** para entenderlo mejor: este se calcula como **1 dividido por la tasa de reserva**.

- Si el banco debe guardar el 10% de cada depósito en reserva, un depósito inicial de \$100,000 podría convertirse en \$1,000,000 al circular por la economía. Eso es porque el multiplicador bancario en este caso sería 10.
- Ahora, si la tasa de reserva baja al 5%, el multiplicador sube a 20. Eso significa que el mismo depósito inicial podría llegar a ser \$2,000,000.
- Si la tasa es solo del 1%, el multiplicador se dispara a 100, haciendo que \$100,000 pueda convertirse teóricamente en \$10,000,000.
- Y si la tasa de reserva es del 0%, no hay un límite definido para cuánto podría crecer ese depósito inicial.

Dato curioso: a partir de 2020, la Reserva Federal (el Banco Central de EE.UU.) redujo los coeficientes de reservas obligatorias al cero por ciento para estimular la economía.



### 3.4 Deuda: la Carga que Aplasta a las Clases Media y Baja



**Deuda** es el dinero que una persona u organización debe a otra. Cuando se tiene una deuda, es necesario devolver el dinero adeudado, normalmente con intereses, en una fecha determinada.

La deuda es un componente crucial en las finanzas modernas, que si se maneja correctamente puede generar crecimiento y estabilidad, pero si se maneja incorrectamente puede dar lugar a crisis financieras. Ya sea para individuos que adquieren una hipoteca para comprar una casa, empresas que buscan expandir sus operaciones, o gobiernos que buscan financiar servicios públicos, la deuda puede actuar como un catalizador de crecimiento. Sin embargo, el manejo imprudente de la deuda puede desencadenar un "círculo vicioso de endeudamiento" o un **"espiral de deuda"** en el que los prestatarios adquieren más deudas para pagar sus deudas existentes.

En este sentido, la tarea de administrar la deuda se vuelve un acto de equilibrio. Por ejemplo, los gobiernos a menudo se endeudan para financiar la infraestructura y los servicios públicos esenciales, contribuyendo así al bienestar y desarrollo de la sociedad. Sin embargo, un endeudamiento excesivo puede llevar a una disminución de la confianza de los inversores, una mayor carga fiscal para las generaciones futuras y una economía en riesgo de caer en una crisis de deuda.

# *Descubriendo el Lado Oscuro del Dinero Fiduciario*

La crisis financiera de Grecia en la década de 2000 proporciona un ejemplo contundente de los peligros de una mala gestión de la deuda. Tras años de gasto deficitario, el país se encontró con una deuda insostenible, desencadenando medidas de austeridad, un fuerte aumento del desempleo y un estancamiento del crecimiento económico. Este caso pone de relieve la importancia del coeficiente **deuda/PIB** como herramienta para evaluar la capacidad de un país para hacer frente a su deuda.

Sin embargo, este coeficiente no es un indicador perfecto. Un coeficiente alto puede sugerir que un país puede tener problemas para pagar su deuda en el futuro, pero un coeficiente bajo no necesariamente significa que un país esté en una posición financiera saludable. También se deben considerar otros factores, como la estructura de la deuda, la fortaleza de la economía y la estabilidad política.

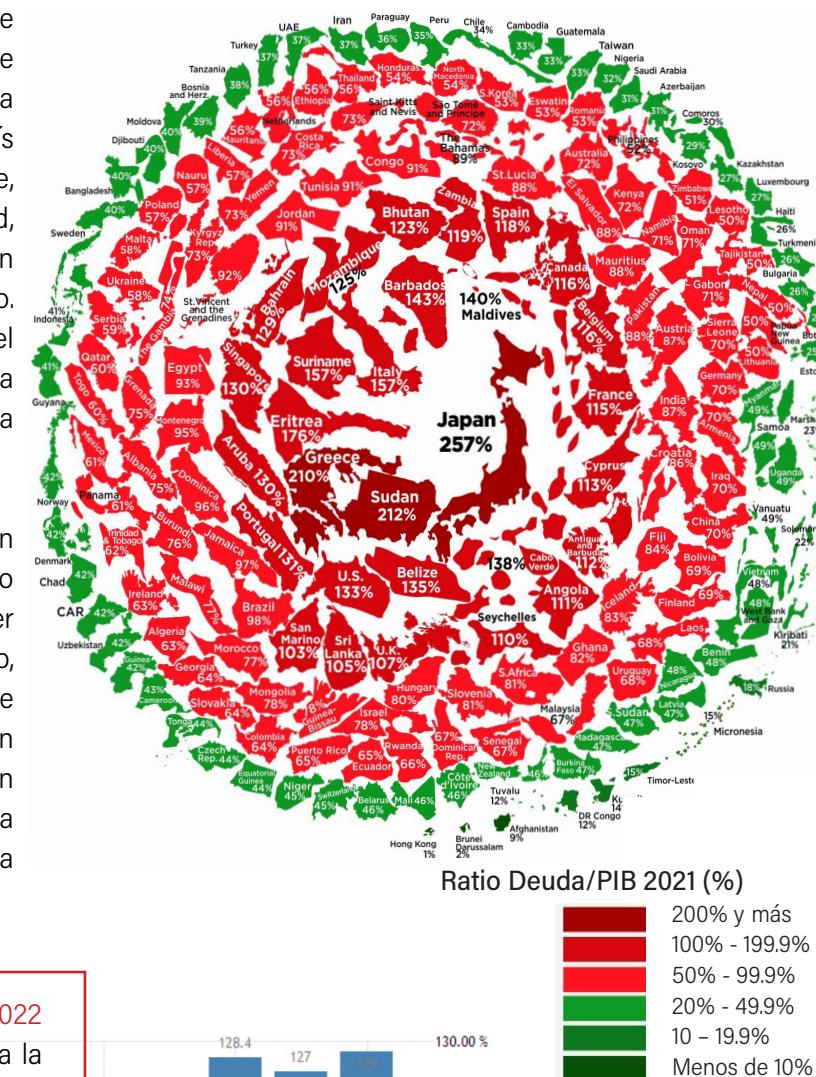
## Ratio de Deuda/PIB de EEUU 2014-2022

Si la deuda sigue creciendo y supera la capacidad del gobierno para manejarla (a través de ingresos fiscales o crecimiento económico), llegará un punto en que el ciclo de deuda será insostenible.



**Producto Interior Bruto (PIB)** es una medida del valor total de los bienes y servicios producidos en un país durante un periodo de tiempo específico, normalmente un año. A menudo se utiliza como indicador del tamaño y la salud de una economía.

## El Estado de la Deuda Pública Mundial





## Capítulo #3

El manejo responsable de la deuda requiere un enfoque multifacético. Los gobiernos, las instituciones financieras y los individuos deben trabajar juntos para crear marcos de préstamo responsables, establecer límites de deuda sensatos y proporcionar educación financiera para fomentar decisiones informadas. Al mismo tiempo, debe haber una mayor transparencia y rendición de cuentas para prevenir la acumulación excesiva de deuda y minimizar los riesgos asociados.

En última instancia, un sistema financiero sano debe estar equipado con mecanismos de alerta temprana y medidas preventivas para detectar y mitigar potenciales crisis de deuda. Como hemos visto, el fracaso en la gestión de la deuda puede tener consecuencias catastróficas, por lo que es esencial adoptar una postura proactiva y prudente en la gestión de la deuda.

### 3.4.1 La Toma de Decisiones

*Ejercicio de Clase :* Escenarios financieros y decisiones a tomar



#### Escenario 1: Decisiones del banco central

El banco central podría subir las tasas de interés para frenar la inflación.

Pregunta: ¿Deberías invertir más en acciones, bonos o guardar el dinero en el banco?

#### Escenario 2: Devaluación de la moneda

Tu país tiene inflación alta y la moneda pierde valor.

Pregunta: ¿Cómo protegerías tu dinero? ¿Lo cambiarías a dólares, comprarías oro, invertirías en propiedades o en bitcoin?

#### Escenario 3: Gasto público

El gobierno quiere gastar más en obras y podría crear más dinero, lo que podría causar más inflación.

Pregunta: ¿Estás de acuerdo con que el gobierno cree más dinero para estos proyectos, o crees que deberían buscar otra manera de pagarlos para evitar más inflación?



# Capítulo #4

## Centralizado vs. Descentralizado: ¿Qué Sistema y Registro es Mejor para Ti?

- 4.0 Los Peligros de la Centralización
- 4.1 El Ascenso de una Sociedad Sin Efectivo
- 4.2 Regulaciones Financieras, Censura y Consecuencias Económicas
  - 4.2.1 Actividad. Consecuencias de la Centralización Digital
  - 4.2.2 El Precio del Control
- 4.3 De la Crisis a la Innovación
  - 4.3.1 Una Comparación entre las Finanzas Centralizadas y Descentralizadas
- 4.4 Una Herramienta Poderosa para Superar las Limitaciones de la Centralización
  - 4.4.1 Las Transacciones son Simplemente Acuerdos para Comerciar
  - 4.4.2 Actividad. El Problema de los Generales Bizantinos y la Descentralización
  - 4.4.3 Del Valor de la Confianza a la Seguridad de las Reglas
- 4.5 "Desencadenando" el Poder de la Cadena de Bloques
  - 4.5.1 La Analogía: Un Vehículo Autónomo

# Centralizado vs. Descentralizado: ¿Qué Sistema y Registro es

## 4.0 Los Peligros de la Centralización



La **centralización**, al concentrar poder e información, puede generar efectos adversos en diversas áreas de la vida. Este modelo puede dar lugar a restricciones, vigilancia intensiva y erosión de la privacidad, limitando la libertad individual y acentuando desigualdades económicas.

Podemos visualizar un sistema centralizado como un árbol robusto, donde el tronco es la autoridad controlando las ramas. Sin embargo, la corrupción del tronco, es decir, la entidad central, puede provocar un cuidado inadecuado de recursos, impactando a todas las ramas y, en particular, a aquellos con menos poder e influencia.



De hecho, el sistema fiduciario moderno se caracteriza por la **centralización del control**, en el que un pequeño grupo de bancos y otras instituciones financieras tienen un peso significativo sobre la economía.

Las autoridades, a través de políticas restrictivas, pueden limitar significativamente las vidas de los ciudadanos. Los controles de capital y las políticas bancarias restrictivas son solo dos formas en las que este control se puede manifestar.

Además, la vigilancia estatal excesiva y la erosión de la privacidad pueden surgir en un sistema centralizado, donde los gobiernos o grandes empresas tienen el potencial de recopilar, almacenar y analizar enormes cantidades de información sobre individuos.

## 4.1 El Ascenso de una Sociedad Sin Efectivo

El avance hacia una sociedad sin efectivo ha tomado un giro importante con la aparición de las Monedas Digitales de los Bancos Centrales (CBDCs). Desde la introducción de las tarjetas de crédito en la década de 1950, hemos abrazado la conveniencia de andar del efectivo. Sin embargo, hay una trampa: cada vez que haces un pago electrónico, hay "intermediarios" que toman una pequeña comisión por cada **transacción**. Tal vez no lo notes porque las cifras son pequeñas, pero sumadas, pueden hacer una gran diferencia. Es algo a tener en cuenta mientras avanzamos hacia un mundo más digitalizado en términos de dinero.

Con las CBDCs, la situación se ha modificado significativamente. Ciertas instituciones gubernamentales ahora pueden tener un registro completo de las actividades económicas de los ciudadanos. Cada **transacción**, sin importar su tamaño, quedaría documentada en una base de datos estatal.

Este nuevo nivel de transparencia puede desencadenar situaciones preocupantes. Los gobiernos podrían penalizar ciertos comportamientos de gasto, restringiendo el acceso a beneficios o servicios. Incluso podrían programar la moneda digital para limitar la compra de productos específicos o deshabilitarla por completo.

Así, con las CBDCs, parece que hemos pasado de pagar una tarifa por el uso de la red a solicitar permiso para usarla. Este control y supervisión intensificados vienen con un coste, ya sea monetario, en privacidad o en autonomía.

A medida que más **transacciones** cotidianas se realizan en línea, el uso de efectivo disminuye. Los gobiernos y los organismos financieros están fomentando los pagos electrónicos y tomando medidas contra el uso de dinero físico. Esto ha desatado un debate sobre el futuro del efectivo y las repercusiones de una sociedad sin dinero físico.



# Centralizado vs. Descentralizado: ¿Qué Sistema y Registro es



La pregunta es: ¿estamos dispuestos a pagar el precio de la comodidad de las finanzas modernas, o buscaremos opciones alternativas que prioricen nuestra libertad y privacidad?

La "guerra contra el efectivo" hace referencia a los esfuerzos por reducir el uso de dinero físico. Mientras algunos argumentan que hará las **transacciones** más rápidas, cómodas y seguras, otros temen una pérdida de privacidad, exclusión financiera y aumento de riesgos de fraude y ciberataques.

Con la llegada de la tecnología digital este debate se ha intensificado. Los defensores de las monedas virtuales argumentan que ofrecen una mayor eficiencia, facilitan la inclusión financiera global y pueden combatir el delito financiero al hacer más difícil el lavado de dinero y la evasión fiscal. Por otro lado, los críticos señalan que la creciente digitalización de las finanzas podría dar lugar a un estado de vigilancia, en el que los gobiernos y las grandes empresas podrían rastrear y controlar todas nuestras **transacciones** financieras.

Además, la transición a una sociedad sin efectivo podría tener consecuencias no deseadas para aquellos que aún dependen en gran medida del efectivo, como las personas mayores, los no bancarizados y aquellos en áreas rurales o menos desarrolladas. Para ellos, el acceso a las **transacciones** digitales puede ser limitado o inexistente.

En las siguientes secciones, profundizaremos en estos aspectos del debate, examinando las razones detrás de la transición hacia una sociedad sin efectivo, los desafíos y preocupaciones que plantea, y las posibles consecuencias para las personas, las empresas y la sociedad en su conjunto.

Desjardins, Jeff. "The Global War on Cash."

Visual Capitalist, 27 Jan. 2017, <https://www.visualcapitalist.com/global-war-cash/>.



## La Guerra Global contra el Efectivo

Hay un impulso global por parte de los legisladores para eliminar el uso de efectivo físico en todo el mundo. Este movimiento a menudo se conoce como "La Guerra contra el Efectivo", y hay tres actores principales involucrados:

- Los Iniciadores
- El Enemigo
- El Fuego Cruzado



P: De qué manera los métodos bancarios convencionales comprometen la seguridad financiera y la privacidad de las personas?

R: Con las tarjetas de crédito, las tarjetas de débito, las transferencias electrónicas y otras redes de pago controladas de forma centralizada, las personas están entregando sus datos de **transacciones** financieras privadas a un tercero y potencialmente sacrificando sus derechos a la privacidad.



**¿QUIÉN?**  
*Gobiernos, bancos centrales*

**¿POR QUÉ?** La eliminación del efectivo facilitará el seguimiento de todo tipo de **transacciones**, incluidas las de delincuentes.



**¿QUIÉN?**  
*Criminales, terroristas*

**¿POR QUÉ?** Las grandes denominaciones de los billetes facilitan la realización de **transacciones** ilegales y aumentan el anonimato.



**¿QUIÉN?**  
*Los ciudadanos*

**¿POR QUÉ?** La eliminación coercitiva del efectivo físico tendrá repercusiones potenciales en la economía y las libertades sociales.

### *¿El efectivo sigue siendo el rey?*

El efectivo siempre ha sido el rey, pero a partir de fines de la década de 1990, la conveniencia de las nuevas tecnologías ha ayudado a realizar **transacciones** que no son en efectivo para volverse más viable:



Hoy en día, existen múltiples formas de pagar digitalmente, que incluyen:



INTERMEDIARIOS



BANCA EN LÍNEA



TELEFONOS



BITCOIN

# Centralizado vs. Descentralizado: ¿Qué Sistema y Registro es



Para 2015, había 426 mil millones de transacciones sin efectivo en todo el mundo - un aumento del 50% con respecto a cinco años antes.



2010

285.2  
MIL MILLONES

426.3  
MIL MILLONES

2015

## Los Primeros Tiros Disparados

El éxito de estas nuevas tecnologías ha llevado a los legisladores a postular que todas las transacciones deberían ser ahora digitales. Aquí está su caso para una sociedad sin efectivo:



*Eliminar la circulación los billetes de alta denominación hace que sea más difícil para los terroristas, traficantes de drogas, lavadores de dinero y evasores de impuestos.*



\$ 1 millón en billetes de \$ 100 pesa solo diez kilogramos (22 libras).

Los delincuentes mueven 2 billones de dólares al año en todo el mundo cada año.

El billete de \$100 USD es el billete más popular del mundo, con 10.000 millones en circulación.



Dinero rastreable significa mayores ingresos fiscales.

También significa que hay un tercero involucrados en todas las transacciones.

Los bancos centrales pueden dictar tasas de interés que fomenten (o desalienten) el gasto para tratar de controlar la inflación.



*Esto da a los reguladores más control sobre la economía.*

*Las transacciones sin efectivo son más rápidas y eficientes.*



Los bancos incurrirían en menos costos al no tener que manejar efectivo.

También facilita el cumplimiento y la generación de informes.

La "carga" de efectivo puede llegar hasta el 1,5% del PIB, según algunos expertos.



Para que esto sea posible, dicen que se debe eliminar el efectivo, especialmente los billetes de alta denominación.



*Después de todo, el efectivo ya sólo se usa para aproximadamente el 16% de todas las transacciones en todo el mundo.*

#### Atrapado en el Fuego Cruzado

Los disparos de los gobiernos que luchan en la guerra contra el dinero en efectivo pueden tener varias bajas no deseadas.



- ▶ Las **transacciones** sin efectivo siempre incluirían algún intermediario o tercero.
- ▶ Ciertos tipos de **transacciones** (juegos de azar, etc.) podrían ser prohibidos o congelados por los gobiernos.
- ▶ Mayor acceso del gobierno a **transacciones** y registros personales.
- ▶ La criptomoneda descentralizada podría ser una alternativa para tales **transacciones**.

Los ahorradores ya no podían tener la libertad individual de almacenar riqueza "fuera" del sistema.

La eliminación del efectivo hace que las tasas de interés negativas sean una opción factible para los políticos.

Significaría que todos los ahorradores estarían "en el anzuelo" de los escenarios de rescate bancario.

Los ahorradores tendrían capacidades limitadas para reaccionar ante eventos monetarios extremos como la deflación o la inflación.



- ▶ La rápida desmonetización ha violado los derechos de las personas a la vida y la alimentación.
- ▶ En India, la eliminación de los billetes de 500 y 1000 rupias ha causado múltiples tragedias humanas, incluida la negación de tratamiento a pacientes y personas que no pueden pagar alimentos.
- ▶ La desmonetización también perjudica a las personas y las pequeñas empresas que se ganan la vida en los sectores informales de la economía.

Con toda la riqueza almacenada de manera digital, aumenta el riesgo potencial y el impacto del delito cibernético.

El hackeo o el robo de identidad podrían destruir los ahorros de toda la vida de las personas.

El costo de las filtraciones de datos en línea alcanza los 2,100 millones de dólares en 2019, según Juniper Research.



# Centralizado vs. Descentralizado: ¿Qué Sistema y Registro es

## 4.2 Regulaciones Financieras, Censura, Vigilancia y Consecuencias Económicas

### Controles de Capital o Sanciones:

Los controles de capital son medidas que los gobiernos implementan para limitar el flujo de divisas fuera del país. Estos pueden manifestarse como restricciones a la cantidad de dinero que los ciudadanos pueden transferir, intercambiar o sacar del país. En tiempos de crisis económica, los gobiernos a veces recurren a estos controles en un intento de estabilizar la economía, aunque a menudo estos esfuerzos terminan intensificando la situación y disminuyendo la calidad de vida de las personas.

Las sanciones, como las impuestas por la Unión Europea a Rusia tras la invasión a Ucrania en 2022, son otro medio por el cual los gobiernos pueden restringir los intercambios financieros. Aunque dirigidas a gobiernos o individuos específicos, estas acciones a menudo tienen efectos colaterales significativos en la economía y el bienestar general de la población.



### Políticas Bancarias Restringidoras:

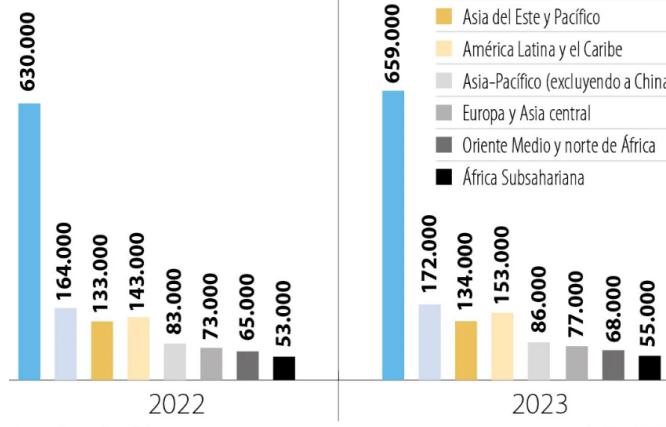
Las políticas bancarias también pueden imponer restricciones significativas a los individuos y las empresas. Esto puede incluir límites de retiro, restricciones de transferencia, altas tarifas por [transacciones](#) y la oferta de préstamos con tasas de interés más bajas a individuos con altos ingresos. Estas políticas pueden exacerbar la desigualdad económica y representar barreras para el acceso a los servicios financieros.

Problemas adicionales pueden surgir debido a los horarios restrictivos de los bancos, la seguridad requerida para acceder a los bancos, los fallos del servidor que interrumpen las [transacciones](#) y las tarifas costosas asociadas con las [remesas](#).



Las [remesas](#) son el dinero que las personas que trabajan en un país envían a sus familias en su país de origen. Si es más difícil y costoso enviar dinero internacionalmente, entonces las personas podrían terminar pagando más para enviar remesas.

PROYECCIONES DE FLUJOS DE REMESAS  
A REGIONES DE INGRESOS BAJOS  
(En millones de US\$)



Fuente: Banco Mundial

Gráfico: LR-GR

**45%** de los hogares no bancarizados poseen criptomonedas, en comparación con



La reciente crisis en Ucrania ha evidenciado cómo los conflictos geopolíticos pueden afectar los sistemas de pago internacionales y los flujos de remesas. Un ejemplo de ello es la exclusión de Rusia del sistema SWIFT, una acción que complicó enormemente las [transacciones](#) financieras, destacando la vulnerabilidad de los sistemas de dinero digital centralizados.

Esta centralización puede resultar en sistemas de pago más fragmentados y menos compatibles entre sí, frenando los avances en la reducción de costos de las remesas, según Dilip Ratha de Knomad. En tales situaciones, los ciudadanos comunes suelen ser los más afectados, ya que pueden encontrarse atrapados en conflictos económicos en los que no están directamente involucrados.

Las remesas representan un salvavidas crucial para muchas familias alrededor del mundo, y cualquier interrupción en estos flujos de dinero puede tener consecuencias devastadoras. Esta fragilidad subraya la importancia de comprender las diferencias y las implicaciones entre las formas centralizadas y descentralizadas de dinero digital.



### La Vigilancia y la Privacidad en la Era Digital

La vigilancia, tanto en su forma física como digital, se ha vuelto un componente omnipresente en nuestra sociedad contemporánea. La era de Internet 4.0, o la Internet de las Cosas (IoT), ha intensificado esta realidad. Con su red de dispositivos interconectados, la IoT recopila enormes cantidades de datos sobre nuestras actividades y preferencias. Aunque estos datos pueden servir para mejorar la experiencia del usuario, también pueden ser utilizados para invadir nuestra privacidad.

En el ámbito físico, las tecnologías de vigilancia, como las cámaras de seguridad, el rastreo GPS y el reconocimiento facial y de voz, también plantean preocupaciones similares sobre la privacidad y la seguridad. Mientras que estas tecnologías pueden ser útiles para prevenir y resolver delitos, también representan una amenaza para la privacidad individual y los derechos civiles.

Una de las ramificaciones más preocupantes de esta tendencia es la capacidad de los gobiernos de utilizar la vigilancia para ejercer control fiscal. Con una visión detallada de las [transacciones](#) de cada individuo, los gobiernos podrían imponer y recaudar impuestos de manera más directa. Podrían incluso desincentivar ciertos comportamientos de gasto al imponer impuestos específicos para esas [transacciones](#), recolectando estos impuestos al instante en el momento de la compra.

Navegar por esta tensión entre seguridad y privacidad requiere un equilibrio delicado y es un desafío constante en la era digital. Debemos tener en cuenta las implicaciones de la vigilancia y los compromisos que podríamos estar haciendo con nuestra privacidad mientras avanzamos en esta era de conectividad y digitalización.

# Centralizado vs. Descentralizado: ¿Qué Sistema y Registro es

El impacto de la IA y la tecnología en la privacidad y la vigilancia del futuro

Efecto futuro	Los ricos	Los pobres
Acceso a información personal	Pueden tener acceso a información personal extensa y pueden usarla para tomar decisiones informadas	Pueden carecer de esta información y tener que depender de fuentes desactualizadas o poco confiables
Capacidad de dar forma al mundo en sus propios intereses	Pueden utilizar su acceso a datos para dar forma al mundo en sus propios intereses	Pueden tener poco influencia en lo que sucede
Control sobre los demás	Pueden ejercer control sobre los pobres a través de su acceso a datos, lo que lleva a una pérdida de libertad individual	Poco control; a menudo son los controlados
Vulnerabilidad a estafas digitales, acoso en línea, extorsión y robo de identidad	Probablemente sean menos vulnerables a estos problemas con más información y más protección contra dichas estafas	Pueden ser más vulnerables a estos problemas debido a la falta de acceso a recursos e información



Una explicación sobre la vigilancia masiva en Internet y sus implicaciones.

## 4.2.1 Actividad: Consecuencias de la Centralización Digital

**Actividad de Clase: Un Mundo con CBDCs.** Sigue las siguientes instrucciones:

### Inicio:

Saca un número al azar para ver cuántos "macarrones" te tocan. Es como el dinero pero en forma de pasta.

### Juega:

- Guarda tus macarrones en el "Banco". Cuidado, podrían cobrarte por guardarlo.
- Compra cosas en el "Mercado". Atento a lo que no puedes comprar.
- Paga "Impuestos" cuando compres algo.
- En el "Centro ESG", toma decisiones buenas y gana más macarrones.
- Si intercambias macarrones entre amigos, podría haber problemas.

### Adáptate:

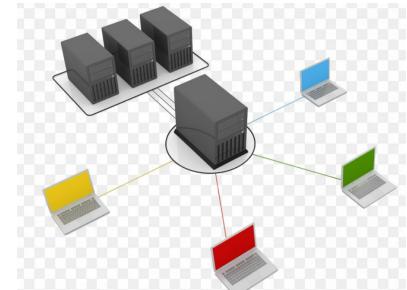
Escucha al profesor. Puede cambiar las reglas o el valor de los macarrones.

### Discute:

Habla en grupo sobre lo bueno y lo malo de tener un sistema de dinero centralizado y digital.

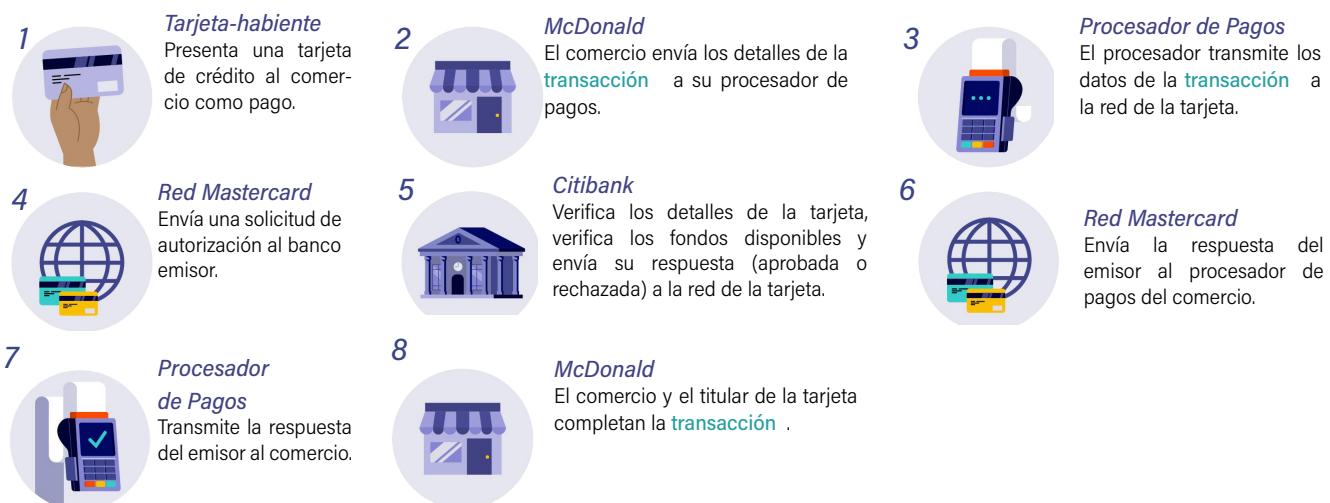
#### 4.2.2 El Precio del Control

A simple vista, el sistema bancario moderno parece sencillo. No obstante, una operación cotidiana como pagar una hamburguesa con tarjeta de crédito implica una serie de intermediarios y costos ocultos. Analizar este proceso nos ayuda a entender las limitaciones y posibles riesgos tras la aparente facilidad.



Los sistemas financieros centralizados, aunque dominantes, encaran retos significativos. Su fragilidad radica en la dependencia de una sola autoridad, concentrando poder excesivo. La necesidad de intermediarios incrementa los costos y reduce la autonomía del usuario. Cuestiones como censura, restricciones, escalabilidad, seguridad y falta de transparencia disminuyen la confianza en el sistema.

Al comprar una hamburguesa con tarjeta, tu pago no pasa directamente del comprador al vendedor. En primera instancia, la operación es procesada por la empresa emisora de tu tarjeta (como Visa o Mastercard), que se lleva una comisión. Luego, la operación es gestionada por tu banco, que también se queda con una comisión por la transferencia de fondos. Posteriormente, los fondos son enviados al banco del vendedor, que cobra otra comisión. Al final, el vendedor recibe el dinero, aunque disminuido por las comisiones en cada etapa.



Entonces, ¿quién asume el costo de todas estas comisiones? Tú, el consumidor, lo haces indirectamente a través del precio de la hamburguesa. ¿Se te notificó de estas comisiones de forma explícita? Lo más probable es que no, ya que estas se incorporan de manera casi imperceptible en el precio final del producto.

Tanto la inflación como la inflación encubierta, ponen de manifiesto las fallas y la ineficiencia inherentes al sistema financiero y bancario tradicional.

# Centralizado vs. Descentralizado: ¿Qué Sistema y Registro es

- Ahora, pasemos a analizar un ejemplo práctico de la administración de **transacciones** en un banco centralizado, como **Citibank**, y cómo pueden surgir desafíos en este sistema. Los libros de contabilidad de los bancos, elementos esenciales para registrar de manera precisa las **transacciones**, son accesibles y manejables únicamente por los integrantes del sistema bancario. Esta característica exclusiva puede desencadenar numerosos problemas y costos innecesarios ligados a la centralización.

Supongamos que el **Citibank** mantiene un libro de contabilidad para tres de sus clientes: A, B y C. Cada uno de ellos inicia con un saldo de \$1000 en sus respectivas cuentas.

Imaginemos que A transfiere \$200 a C. En una operación normal, el libro de contabilidad se actualizaría para reflejar la **transacción**, restando \$200 del saldo de A y agregando los \$200 al saldo de C.

Pero, ¿qué ocurre si debido a un error humano o del sistema la **transacción** se registra duplicada? En tal escenario, se sustraerían \$400 de la cuenta de A y se añadirían \$400 a la cuenta de C. Esta situación no refleja la realidad, ya que la transferencia original debía ser solo de \$200. Esta incongruencia pone de manifiesto el riesgo de **duplicidad** en las **transacciones**.

Pero, ¿qué sucede si C luego efectúa una compra por valor de \$1300? Si se toma en cuenta la **transacción** incorrectamente duplicada, C tendría fondos suficientes para realizar la compra. Sin embargo, si posteriormente se detecta y corrige el error, la cuenta de C se encontraría con un déficit. Esta situación ilustra cómo un error de duplicación puede conducir a saldos incorrectos y potencialmente a deudas insostenibles.

Aquí es donde los inconvenientes de la centralización se vuelven evidentes. En este modelo, Citibank posee un control absoluto sobre el libro de contabilidad y es el único capaz de rectificar errores. Si dichos errores pasan inadvertidos, los efectos para los clientes podrían ser perjudiciales.

Si este error no fuera un descuido sino una acción intencionada, ¿cómo podría evitarse la manipulación del libro de contabilidad? En el caso de Bitcoin, que opera en una red descentralizada, la seguridad se eleva a otro nivel. Todas las transacciones se registran en múltiples nodos distribuidos por la red. Para alterar el libro de contabilidad, sería necesario obtener el consenso de más de la mitad de estos nodos. Este requisito crea una barrera significativa contra intentos de manipulación, proporcionando una capa adicional de seguridad.

Cliente	Saldo
A	\$1000
C	\$1000
D	\$1000

Cliente	Saldo
A	\$800
C	\$1200
D	\$1000

Cliente	Saldo
A	\$600
C	\$1400
D	\$1000



### 4.3 De la crisis a la innovación



Mucho antes del surgimiento de **Bitcoin**, existía un deseo persistente de abordar los desafíos asociados con el sistema financiero tradicional, como el fraude, la corrupción y la creciente desconfianza en las instituciones financieras. Con la crisis financiera mundial de 2008, estos problemas se acentuaron aún más.

Un grupo de visionarios técnicos, conocidos como los Cypherpunks, ya se encontraban explorando soluciones alternativas. Este movimiento, nacido en la década de los 90, estaba compuesto por programadores y activistas apasionados por la potencialidad de la **criptografía** para impulsar cambios sociales positivos y redefinir las relaciones de poder tradicionales.

Inspirados por la filosofía libertaria y los ideales de privacidad y seguridad digital, los Cypherpunks se dedicaron a experimentar con el concepto de una **moneda digital** que pudiera ser utilizada en **transacciones** en línea sin la necesidad de intermediarios, como los bancos.



"Wired" es una revista estadounidense que se enfoca en cómo las tecnologías emergentes afectan la cultura, la economía y la política. Fue fundada en 1993 por Louis Rossetto y Jane Metcalfe.

Antes de **Bitcoin**, existieron varios intentos por crear monedas digitales, como b-money de Wei Dai y Bit Gold de Nick Szabo. A pesar de que estos proyectos no lograron una implementación a gran escala debido a diversos obstáculos, las tecnologías e ideas que emergieron de ellos jugaron un papel crucial en la concepción de **Bitcoin** como una alternativa transparente y descentralizada.

Así, la descentralización, concepto central en la filosofía de los Cypherpunks, se convirtió en una solución clave en la creación de **bitcoin**, una moneda digital revolucionaria que prometía cambiar nuestra concepción del dinero y las **transacciones** financieras. Para llevar a cabo esta visión, era necesario desarrollar una forma de registrar las **transacciones** que fuera más segura, transparente y resistente a la corrupción que los sistemas de libros de contabilidad centralizados tradicionales.

#### 4.3.1 Una Comparación entre las Finanzas Centralizadas y Descentralizadas



A medida que navegamos en la transición hacia una sociedad sin efectivo, es vital comprender la diferencia entre la digitalización del dinero centralizado y el descentralizado. Aunque ambos se refieren a formas de dinero que existen en formato digital, hay diferencias significativas en su estructura y control que pueden tener un impacto profundo en nuestras finanzas y privacidad.

A medida que avanzamos hacia una sociedad cada vez más digital, es crucial entender estas disimilitudes y soportar las ventajas y desventajas que cada sistema puede aportar. Esta comprensión informada nos permitirá tomar decisiones financieras más seguras y conscientes en un mundo cada vez más digital y conectado.

# Centralizado vs. Descentralizado: ¿Qué Sistema y Registro es

## 4.3 Una Herramienta Poderosa para Superar las Limitaciones de la Centralización

Los sistemas descentralizados se asemejan a un bosque, un lugar donde cada árbol simboliza un participante independiente, y el bosque la totalidad del sistema. En esta analogía, el bosque es más resistente que un solo árbol, ya que no depende de un sólo punto de fallo. Si un árbol se daña, el bosque puede seguir prosperando. Los sistemas descentralizados, como los bosques, son más eficaces con participantes diversos y colaborativos, en lugar de una única autoridad central dictando las reglas.



Ventajas de los sistemas descentralizados:

- Mayor resistencia y fiabilidad al no existir puntos únicos de fracaso.
- Mayor protección mediante el cifrado adecuado, dado que no existe un punto principal de control para los piratas informáticos.
- Mayor soberanía por parte de los participantes, quienes tienen más control sobre los recursos y las decisiones.
- Mayor transparencia, ya que todos los nodos acceden a la misma información en la red.
- Sin permisos y sin límites, lo que significa que cualquiera puede unirse, influir y/o participar.
- Mayor privacidad y seguridad mediante el uso de seudónimos o apodos.



Un **nodo** es un *computador conectado a una red* que puede *compartir y/o recibir información* y comunicarse con los demás nodos.

Desafíos de los sistemas descentralizados:

- Mayor esfuerzo necesario para lograr el consenso entre los **nodos**.
- Mayor vulnerabilidad ante nodos maliciosos que podrían dañar la **red**.



Una **red** es un grupo de **nodos** que están conectados unos a otros de una forma u otra. Esta conexión les permite intercambiar información y estar comunicados entre sí.

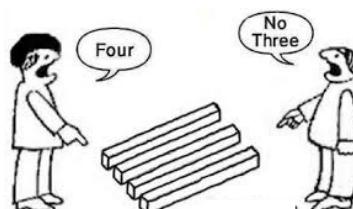
En las redes descentralizadas, las **transacciones** ocurren de manera directa, de persona a persona (también conocido como modelo **Peer-to-Peer** o P2P), eliminando la necesidad de intermediarios. En lugar de pasar por una entidad centralizada, como un banco o un proveedor de servicios de pago, las **transacciones** en una red descentralizada se realizan directamente entre los usuarios.



#### 4.4 Las **Transacciones** son Simplemente Acuerdos para Comerciar

**Piedras Rai**

¡Bienvenidos a la isla Micronesia descentralizada de Yap! Es un lugar un poco remoto, pero fascinante porque las personas usan un tipo especial de moneda llamada "Piedras Rai". Una característica que las convierte en una excelente forma de dinero es su escasez. El número total de Piedras Rai es limitado, lo que significa que no pueden ser fácilmente reproducidas o infladas como las monedas fiduciarias. Esta oferta fija ayuda a mantener el poder adquisitivo de las Piedras Rai con el tiempo y las convierte en una tienda de valor confiable. Estas Piedras Rai son como monedas gigantes que se usan para comprar cosas en la isla. El problema es que pueden pesar una tonelada. Las Piedras Rai pueden aplastarte, por lo que son un poco imprácticas para llevar a cuestas. ¿Cómo, entonces, pueden las personas usar cómodamente las Piedras Rai como medios de intercambio sin tener que moverlas físicamente de un lugar a otro?



#### Confiar o No Confiar

Aunque el dólar estadounidense es ahora la moneda oficial de la isla de Yap, las Piedras Rai siguen siendo un tipo de dinero. A diferencia de los dólares, las Piedras Rai en la isla de Yap no están controladas por una única autoridad ni almacenadas en bancos. En lugar de eso, las **transacciones** se basan en historia oral y confianza, con las personas llevando la cuenta de sus propios registros de quién posee qué piedras. Este sistema, que ha existido como uno de los primeros intentos documentados de crear un sistema que es auditável y visible para todos sin una autoridad central, se basa en consenso social y cultural. Este tipo de **transacción**, donde ninguna moneda se entrega físicamente de un individuo a otro como forma de pago, sino que un objeto físico se usa como símbolo de valor, es común en la isla de Yap y se ha utilizado durante siglos como forma de moneda.

Este sistema tiene tanto beneficios como inconvenientes. Por un lado, permite cierto grado de independencia de una autoridad central. Por otro lado, también puede llevar a desacuerdos y potencial para hacer trampa. ¿Por qué?

Considera este dilema: Raquel intercambió una piedra rai con Natalia por un bote hace años. Hoy, Raquel afirma que nunca entregó la piedra. En una sociedad que se basa en la memoria colectiva, estos conflictos pueden ser complicados de resolver.

# Centralizado vs. Descentralizado: ¿Qué Sistema y Registro es

Entonces, ¿cómo pueden miles de personas, que no se conocen entre sí, ponerse de acuerdo sobre qué **transacciones** son válidas sin tener una autoridad central? Aquí es donde la tecnología entra en juego. Usando programación e internet, se ha creado un sistema donde cada **transacción** se guarda de forma segura y no se puede cambiar. Esto hace que todos estén de acuerdo en lo que es verdad y lo que no, sin necesidad de un jefe o una autoridad central que lo decida.

## 4.4.2 Actividad de Clase: El Problema de los Generales Bizantinos y la Descentralización

Objetivo: Llegar a un consenso sobre si se debe "Atacar" o "Retirar", incluso cuando algunos mensajeros puedan estar entregando información falsa.

### Materiales:

- Muñequeras o cintas de colores (**doradas para los Generales, azules para los mensajeros**).
- Sobres sellados con mensajes: "**Atacar**" o "**Retirarse**".
- Banderas rojas y blancas para Generales.



### Roles:

- 2-4 Generales
- Varios mensajeros (número equitativo por cada General)

### Inicio:

General A recibe un mensaje y lo transmite a sus mensajeros individualmente.  
Se elige aleatoriamente a algunos mensajeros para ser traidores.

### Comunicación entre Mensajeros:

Los mensajeros pueden compartir el mensaje con otros mensajeros, ya sea del mismo General o de otro.

### Recuerda:

Un mensajero solo puede transmitir el mensaje una vez a otro mensajero específico.

### Comunicación con Generales:

Los mensajeros transmiten el mensaje a sus Generales respectivos.  
Los Generales no pueden hablar entre sí.

### Decisiones:

Después del período de comunicación, cada General decide si "Ataca" o "Se Retira" y elige la bandera correspondiente.

Los Generales revelan sus decisiones simultáneamente.

#### 4.4.3 Del Valor de la Confianza a la Seguridad de las Reglas

Imagina que estás en un chat grupal con amigos. En lugar de intercambiar bienes, simplemente hablan y hacen planes. Cada mensaje enviado queda registrado para que todos puedan verlo.

##### Sistema Descentralizado y Seguridad

Todos en el chat tienen acceso al historial completo de mensajes. Si alguien intenta cambiar un mensaje antiguo, el grupo se dará cuenta inmediatamente. Este nivel de transparencia es similar al de una **cadena de bloques** como la de **Bitcoin**.

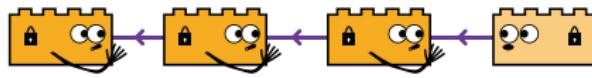
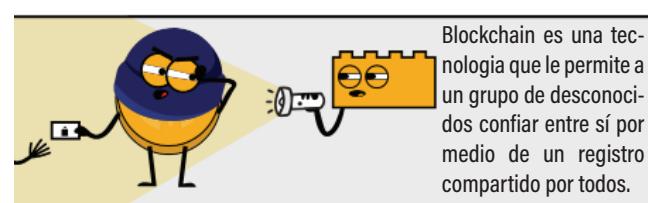
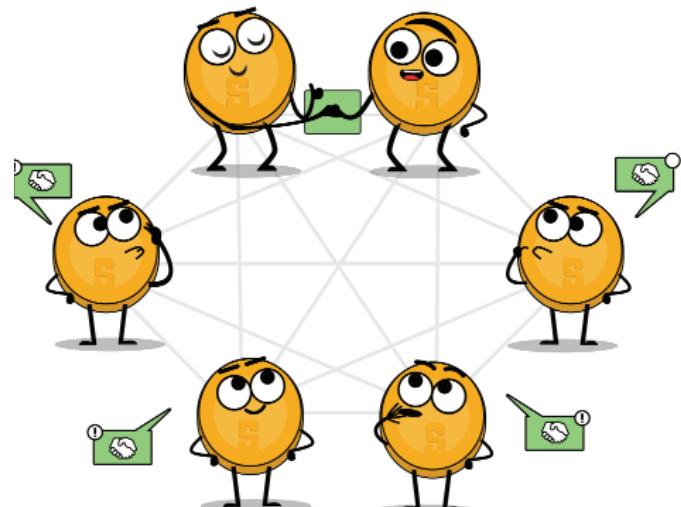
En un sistema descentralizado, no necesitas confiar en una única persona o entidad. En lugar de eso, confías en un conjunto de reglas acordadas por todos. Estas reglas garantizan que la información sea segura y precisa.

##### Aplicación a la Isla de Yap

Si la Isla de Yap hubiera tenido un sistema descentralizado con reglas claras y un registro público, se habrían evitado muchos conflictos. Cada **transacción** con Piedras Rai habría quedado registrada, eliminando dudas sobre quién es el dueño legítimo de cada piedra.

¿Pero es realmente así de simple? No exactamente; hubo mucho de prueba y error antes de que la tecnología de la **cadena de bloques** fuera realmente un éxito.

- ¿Cuáles son las reglas exactas a seguir?
- ¿Quién establece estas reglas?
- ¿Por qué querrán las personas seguir las reglas?
- ¿Cómo se distribuyen las reglas en la red?
- ¿Qué sucederá si alguien rompe las reglas?
- ¿Cómo se pueden cambiar o actualizar las reglas más adelante?
- ¿Cómo se harán cumplir las reglas para asegurar que todos las sigan?
- ¿Cómo se pueden hacer las reglas claras y fáciles de encontrar para todos en el sistema?



# Centralizado vs. Descentralizado: ¿Qué Sistema y Registro es

## 4.5 "Desencadenando" el Poder de la Cadena de Bloques

Desde los 90, la idea de tener un sistema de registro descentralizado rondaba en el aire, pero no se hizo realidad hasta que Satoshi Nakamoto creó **Bitcoin** en 2008. Usando una técnica que estudiaremos más adelante, Nakamoto logró que todos pudieran ponerse de acuerdo en quién posee qué sin necesitar un intermediario de confianza. Esto no solo cambió nuestra forma de ver el dinero, sino que también abrió puertas a una nueva era de independencia financiera y control individual.



Un **blockchain** es como un libro de contabilidad digital que todos pueden ver pero nadie puede alterar fácilmente. En él se registran todas las **transacciones** o datos en unidades llamadas bloques. Estos bloques están encadenados y protegidos con medidas de seguridad. Lo que lo hace especial es que no está guardado en una sola computadora ni controlado por una sola organización, lo que lo hace más seguro y transparente.

1 Garantiza que la información esté disponible en cualquier momento.

**Disponibilidad**



2 El registro es consensulado: cada nodo almacena la misma información.

**Integridad**



3 Como cada bloque está vinculado al anterior, la cadena no se puede alterar.

**Inmutabilidad**



Todos los registros de acciones en la **blockchain** (**cadena de bloques**) se denominan **transacciones**.

El verdadero valor de la **blockchain** no está solo en la tecnología misma, sino en su capacidad para crear redes que son abiertas y no controladas por una sola entidad. Estas redes nos permiten hacer negocios e interactuar de una forma que da más poder a las personas, algo que siempre fue el objetivo de **Bitcoin**.

### 4.5.1 La Analogía: Un Vehículo Autónomo

**Bitcoin**- es comparable a un vehículo autónomo en el ámbito financiero. A diferencia de los primeros sistemas de **transacción** digital, que requerían de un 'conductor' como un banco o un gobierno, **Bitcoin** opera de forma autónoma. Está diseñado para ofrecer libertad financiera mediante **transacciones** seguras, rápidas y eficientes, sin la necesidad de intermediarios, incluso cuando se trata de cruzar fronteras internacionales.



**Sistema de Piloto Automático (Reglas de Consenso)**-Este es como el cerebro del carro, el que sigue **reglas** estrictas para que todo funcione de forma segura y eficiente. Asegura que cada "pasajero" (**transacción**) llegue a su destino correcto, consultando con otros carros en la red si hay dudas sobre qué camino tomar.

**El GPS con Odómetro Avanzado - Blockchain (Cadena de Bloques)**: Este GPS no solo guía el camino sino que también registra cada "viaje" o **transacción**, mostrando desde dónde y hacia dónde se movió cada **bitcoin**. Este registro es público y seguro.

**El Sistema de Transmisión - Red Peer-to-Peer**: Son las "carreteras" por donde viaja el vehículo. Facilitan el movimiento de **bitcoins** entre los usuarios, como si fueran carros viajando por la misma red de carreteras.

**Combustible - Mineros**: Los mineros son como el combustible especial que permite que el sistema de piloto automático y el motor funcionen correctamente. Añaden nuevos "viajes" al GPS con Odómetro Avanzado (**Blockchain**).

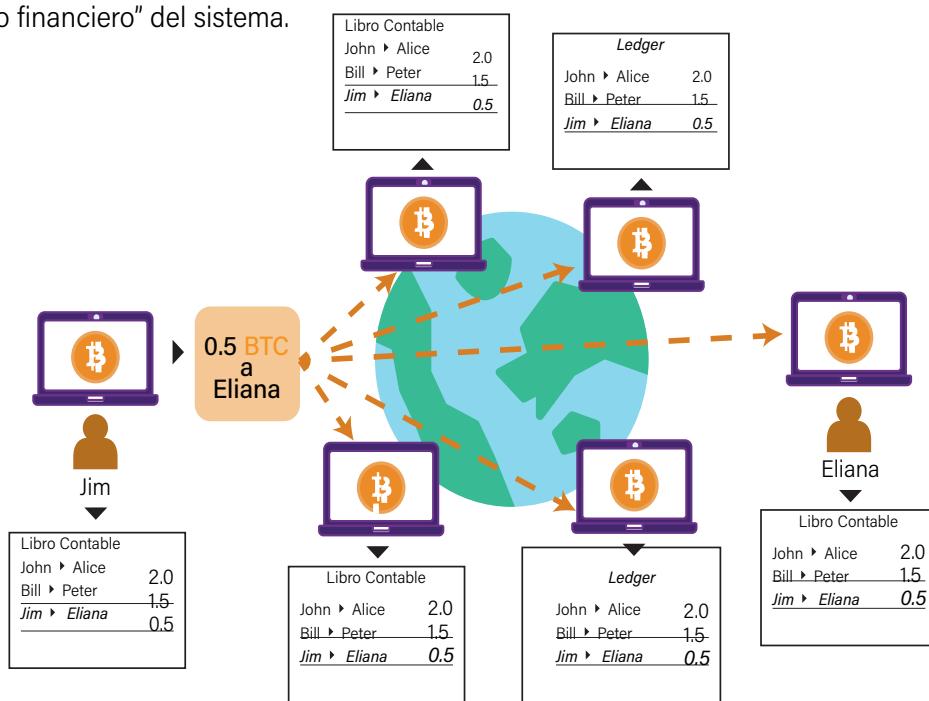
**Pasajeros - Usuarios**: Los usuarios son como los pasajeros que deciden a qué "destinos financieros" quieren ir. Realizan **transacciones** pero no se encargan del mantenimiento del carro (minado).

### La Prueba de Carretera: Cómo el Carro Autónomo de Bitcoin Resuelve Conflictos

Supongamos que hay una **transacción** en la cual Jim afirma haber enviado a Eliana **0.5 BTC**. Eliana, sin embargo, niega haber recibido esta cantidad. ¿Cómo se resuelve el conflicto? Ambos pueden consultar la **blockchain**, que actúa como el "GPS con odómetro financiero" del sistema.

Si el registro muestra que Jim envió **bitcoins** a Eliana, entonces Jim tiene razón. Si no hay registro, Eliana tiene razón. Gracias al sistema de piloto automático, no necesitan una "policía de tráfico" (banco o gobierno) para resolver el problema.

Al priorizar una verdadera descentralización y alinearnos con los principios de **Bitcoin**, podemos crear un futuro que empodere a los individuos y promueva una mayor libertad e igualdad.





# Capítulo #5

## El Futuro del Dinero Sólido: Introducción al Bitcoin

5.0 La Revolución Financiera

5.1 ¿Qué es bitcoin? ¿Qué es Bitcoin?

5.1.1 ¿Cuál es la diferencia entre bitcoin y Bitcoin?

5.1.2 ¿Para qué aprender sobre bitcoin si me es imposible pagarlo?

5.1.3 ¿De qué está hecho el bitcoin?

5.1.4 ¿Cómo recibes bitcoins?

5.1.5 ¿Cómo utilizo por primera vez?

5.1.6 ¿Cómo puedo enviar o transferir bitcoin de un monedero a otro?

5.1.7 ¿Qué me impide duplicar el mismo bitcoin y enviarlo a varias personas?

5.1.8 ¿Cómo ingresan nuevos bitcoins a la red?

5.1.9 ¿Se puede apagar o prohibir Bitcoin?

5.2 ¿Quienes son los Protagonistas de Bitcoin?

5.3 ¿Cómo Funciona una Transacción de bitcoin en Bitcoin?

5.3.1 Actividad. Transacciones en Acción

5.4 Un Nuevo Enfoque al Dinero

5.4.1 ¿Cual es la Mayor Diferencia entre Bitcoin y la Banca Tradicional?

5.4.2 Evaluando el Consumo Energético: Bitcoin frente a la Banca y la Minería Tradicionales

5.5 ¿Son Seguras las Transacciones de bitcoin?

# El Futuro del Dinero Sólido: Introducción al Bitcoin

## 5.0 La Revolución Financiera

Ahora que hemos abordado la tecnología **blockchain** y su importancia en sistemas descentralizados, centrémonos en **Bitcoin**. Vamos a examinar su esencia, su funcionamiento y lo que le otorga valor, diferenciándolo así de otras monedas y de otros sistemas financieros. A lo largo de este capítulo, examinaremos las **transacciones** en

**bitcoin**, los roles clave dentro de su red y un caso práctico para ilustrar su desempeño. También indagaremos en el misterio en torno a su creador(a), **Satoshi Nakamoto**. Al concluir, tendrás un entendimiento sólido de los fundamentos de **Bitcoin** y podrás considerar su potencial impacto en el futuro.



**Bitcoin** está en esa lista de las cosas que prometen transformar el mundo por completo. En este video se explica que es **Bitcoin** y como funciona.



¿Cuando, por qué y quién creó **Bitcoin**?

En el contexto de la crisis financiera de 2008, una persona o grupo bajo el seudónimo Satoshi Nakamoto lanzó **Bitcoin**. Publicando el **whitepaper** en octubre de 2008 en una lista de correo de Cypherpunks, activistas pro-criptografía y privacidad, Satoshi respondió a la desconfianza creciente en las instituciones financieras.



Un **whitepaper**, también conocido como informe técnico, es un documento que actúa como una guía exhaustiva sobre un tema específico, normalmente con el objetivo de resolver un problema o explicar una nueva tecnología.



**Bitcoin:** Un sistema de efectivo electrónico de usuario a usuario.



Sólo contiene 9 páginas

El **whitepaper** de **Bitcoin** describió cómo funcionaría **Bitcoin** y cómo solucionaría problemas en el dinero digital. Sirvió como una guía para que la gente entendiera la idea detrás de **Bitcoin** y cómo usarlo de manera segura.

**Bitcoin** se propone como una moneda digital descentralizada, a prueba de fraude y con suministro limitado. Elimina intermediarios y guarda todas las **transacciones** en un registro público e inmutable. La desconfianza de Satoshi hacia el sistema financiero se refleja en su primer mensaje en la **blockchain**, que cita un artículo del periódico **The Times** sobre un posible segundo rescate bancario.



## Capítulo #5

Los datos documentados sobre Satoshi Nakamoto son limitados y principalmente se basan en los escritos y acciones realizadas bajo este seudónimo. Aquí hay algunos puntos clave:

- **Creación del Software de Bitcoin:** Nakamoto lanzó la primera versión del software de Bitcoin en 2009 bajo un código abierto y minó el primer bloque de la blockchain, conocido como el bloque génesis.
- **Comunicación en Foros:** Nakamoto participó activamente en foros en línea y listas de correo electrónico para discutir y mejorar Bitcoin, hasta aproximadamente finales de 2010 o principios de 2011.
- **Desaparición:** Nakamoto gradualmente se retiró de la comunidad Bitcoin, delegando responsabilidades a un grupo de desarrolladores. Desapareció en 2011, dejando un mensaje que decía que se había "movido a otras cosas".
- **Estimación de bitcoins Poseídos:** Se estima que Nakamoto podría tener alrededor de 1 millón de bitcoins que nunca han sido movidos desde sus direcciones de billetera.
- **Multidisciplinario:** Los escritos de Nakamoto abarcan temas desde la criptografía hasta la teoría de juegos y economía, lo que lleva a la especulación de que podría ser un grupo de personas con conocimientos en diversas disciplinas.
- **Inglés Neutro:** El inglés utilizado por Nakamoto en sus comunicaciones y en el white paper es neutro, lo que hace difícil determinar su origen geográfico.
- **No se menciona "Blockchain":** Aunque es el creador de la primera cadena de bloques, el término "blockchain" no aparece en el white paper original.
- **Foco en Descentralización:** Uno de los temas recurrentes en los escritos de Nakamoto es el poder de la descentralización y el objetivo de crear un sistema financiero que no dependa de intermediarios.
- **Anonimato y Privacidad:** Nakamoto puso énfasis en estos aspectos, tanto en el diseño de Bitcoin como en su propia identidad.

### *Preguntas que Satoshi podría haberse planteado al diseñar Bitcoin*



- ¿Cómo evito que alguien use la misma moneda dos veces?
- ¿Cómo sé que la persona con la que estoy haciendo negocios en línea es realmente quien dice ser?
- ¿Cómo me aseguro de que alguien tiene suficiente dinero digital para pagarme?
- ¿Cómo logro que un grupo de computadoras se ponga de acuerdo para tomar decisiones justas?
- ¿Puede funcionar un sistema así aunque no todos sean honestos?
- ¿Quién tiene acceso a una copia de toda la cadena de datos?
- ¿Cuáles son las transacciones que se pueden realizar?

# El Futuro del Dinero Sólido: Introducción al Bitcoin

Aunque Satoshi ha permanecido en el anonimato, su invención ha causado un impacto mundial, desafiando los sistemas financieros preexistentes e inspirando innumerables adelantos en el espacio digital.

El 22 de mayo de 2010, se realizó la primera **transacción** de **bitcoin** por un bien tangible: dos pizzas por 10,000 BTC. Este evento, ahora conocido como el “Día de la Pizza **Bitcoin**”, demostró que **Bitcoin** no es solo un experimento; es un **medio válido de intercambio y almacenamiento de valor**. Desde ese momento, el vehículo autónomo de **Bitcoin** ha estado circulando por las carreteras del mundo financiero, llevándonos a destinos que antes eran inimaginables sin la necesidad de un ‘conductor’ o autoridad central.

## 5.1 ¿Qué es **bitcoin**? ¿Qué es **Bitcoin**?



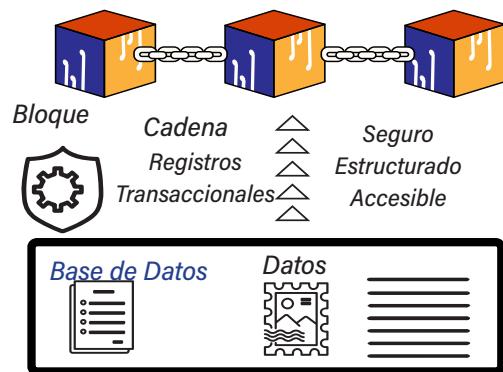
**bitcoin** es la moneda digital que utilizas. **Bitcoin** es el sistema descentralizado que permite que esa moneda funcione, basado en la tecnología **blockchain** que registra todas las **transacciones**.



### ¿Qué es **bitcoin**?

**bitcoin**, con “b” minúscula, es una forma de dinero virtual. Aunque puedes usarlo para adquirir productos o servicios tanto en línea como en establecimientos que lo aceptan, no existe en forma física. En lugar de tener billetes o monedas en una cuenta bancaria, lo que tienes son registros digitales de **transacciones** almacenadas en una red de computadoras.

### ¿Qué es la **blockchain** de **Bitcoin**?



### Bitcoin como sistema de pago

**Bitcoin** es especial porque, a diferencia de las monedas tradicionales, no está controlado por ningún banco o gobierno. Esto lo hace un sistema descentralizado, permitiendo a las personas enviar y recibir **bitcoins** directamente entre sí, sin la necesidad de un intermediario como un banco. Cada **transacción** entre pares queda grabada en una **base de datos** pública conocida como la **blockchain** de **Bitcoin**.

### La red **Bitcoin**

Cuando hablamos de **Bitcoin** con “B” mayúscula, nos referimos a toda la tecnología que hace posible el uso de **bitcoin**. Son muchos computadores interconectados usando el mismo software quienes la componen.

### Bitcoin como un movimiento

**Bitcoin** es más que sólo una forma de dinero digital. Es también un movimiento de gente que quiere tener más control sobre su dinero. Cualquier persona puede unirse a la red **Bitcoin**. No necesitas permiso, sólo necesitas una computadora y acceso a internet.



## Capítulo #5

### 5.1.1 ¿Cuál es la diferencia entre bitcoin y la red Bitcoin?

Una forma de entender la asociación entre **bitcoin** y la **red Bitcoin** es compararla con la existente entre un **correo electrónico** e **Internet**. Así como un correo electrónico es un mensaje que se guarda, se envía y se recibe a través de Internet, **bitcoin** es una **moneda** digital que se transfiere y se recibe a través de la **red Bitcoin**. El Internet proporciona la infraestructura para que los correos electrónicos se envíen y se reciban al mismo tiempo, la **red Bitcoin** proporciona la **infraestructura** para que **bitcoin** se transfiera y se reciba.

Correo Electrónico / bitcoin



Internet / Red Bitcoin

### 5.1.2 ¿Para qué aprender sobre bitcoin si me es imposible pagarlo?

¿Te has planteado alguna vez la posibilidad de usar **bitcoin**, pero te ha desanimado el precio elevado de un **BTC**? No te preocupes, ¡no eres el único! La buena noticia es que no tienes que comprar un **bitcoin** entero. Del mismo modo que existen fracciones de dólar (hasta centavos), también existen fracciones de **bitcoin**. Si lo que quieras es comenzar invirtiendo \$1USD en **bitcoin**, lo puedes hacer sin problema.



El símbolo de **bitcoin** es **BTC** o **B** y la abreviatura de **satoshis** es **sats** de forma similar a como un dólar es USD o **\$**.

La conversión es:

**1 BTC = 100,000,000 sats**

Un **bitcoin** es divisible en 100 millones de unidades llamadas **satoshis**, y por tanto puedes comprar cualquier cantidad de **bitcoin**, aunque sea pequeña. Ahora que sabes que puedes cambiar tan sólo unos pocos centavos por una fracción de **bitcoin**, ¡vamos a explorar las posibilidades de uso de esta moneda digital!

Imagina que deseas comprar una manzana que cuesta \$1.40, pero aún no tienes **bitcoin**. No te preocupes, incluso si solo tienes una pequeña fracción de **bitcoin**, como 0.00008 **bitcoin** (equivalente a 8000 **satoshis**), podrás realizar la compra. Después de pagar en la tienda, si revisas tu saldo en tu monedero, es probable que aún te queden algunos **satoshis**, incluso podrías haber guardado el cambio. Esto demuestra que no necesitas tener un **bitcoin** completo para comenzar a usarlo, ya que incluso una pequeña fracción es suficiente para hacer **transacciones**. Pero entonces, ¿dónde se guarda ese cambio?

Satoshi	Bitcoin
1	0.00000001
10	0.00000010
100	0.00000100
1,000	0.00001000
10,000	0.00010000
100,000	0.00100000
1,000,000	0.01000000
10,000,000	0.10000000
100,000,000	1.00000000

A medida que más personas usan **bitcoin** para pagos cotidianos, usar **sats** podría ser más práctico.

# El Futuro del Dinero Sólido: Introducción al Bitcoin



Los monederos, billeteras o carteras de **bitcoin**, que pueden funcionar simplemente como aplicaciones en tu dispositivo móvil, actúan como custodios o guardianes digitales que garantizan el acceso seguro a tus **bitcoins**. Estas billeteras son comparables a bóvedas personales digitales que almacenan información crucial sobre la posición actual de tus **bitcoins** y su historial de **transacciones**.

## 5.1.3 ¿De qué está hecho el **bitcoin**?

Al igual que los billetes de dólar se pueden rastrear mediante sus números de serie, en el mundo digital se da más importancia a rastrear las **transacciones** que a las unidades de dinero en sí. Esto es cierto tanto para sistemas centralizados como los bancos, como para sistemas descentralizados como **Bitcoin**.

Cada vez que haces una **transacción** con **bitcoin**, se crea un código único que la identifica y la rastrea y funciona como la "huella digital" de esa operación. Este código detalla quién envió o recibió el **bitcoin** y en qué cantidad. Todas estas **transacciones** quedan registradas en un libro digital que es visible para todos y que no puede ser alterado, conocido como la **cadena de bloques** o "**blockchain**" y en el contexto de **Bitcoin**, también se le llama '**timechain**' o **cadena de tiempo** para enfatizar el rol crucial del tiempo y el orden en el sistema.



El **bitcoin** se compone de datos y su valor proviene de su autenticidad, su escasez, y seguridad.



**Número de Serie:** es una combinación única de números y letras que identifica un objeto o producto específico. En el caso de un billete, aparece dos veces en el frente del mismo.



=      =  
79054025255fb1a2  
Wally le **envió** 3000 **sats** a Carlos a las 10:00 am el 4/16/23

Cada **transacción** de **bitcoin** tiene una huella digital única que indica cuánto dinero se transfiere, de dónde viene y a dónde va.

## 5.1.4 ¿Cómo recibes **bitcoins**?

Existen diversas formas de obtener **bitcoins**, como comprarlos en casas de cambio (en línea), recibirlos como regalo o pago por bienes y servicios, o incluso minarlos (\*entenderás más adelante) con una computadora especializada. Independientemente del método que elijas, una vez que hayas obtenido tus **bitcoins**, los almacenarás en un monedero digital, el cual te permite guardar, recibir y enviar **bitcoins** de forma segura.



Aquí encontrarás las múltiples opciones.

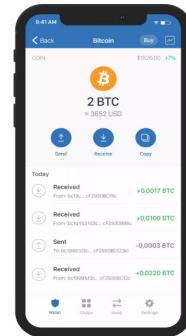


## Capítulo #5



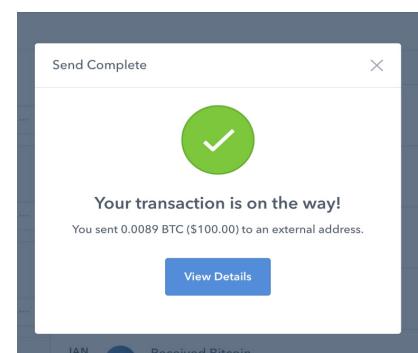
### 5.1.5 ¿Cómo utilizo bitcoin por primera vez?

Para empezar a usar **bitcoin**, primeramente tendrás que obtener un monedero digital. Esto es similar a instalar una aplicación de pago como Venmo, CashApp o Apple Pay en tu dispositivo o smartphone. Tu monedero digital te permitirá guardar tus **bitcoins**, así como enviar y recibirlos de otras personas, e incluso comprar bienes y servicios en línea. Por lo tanto, necesitas un monedero digital para llevar a cabo **transacciones** con **bitcoin**.



### 5.1.6 ¿Cómo puedo enviar o transferir bitcoin de un monedero a otro?

Enviar o transferir **bitcoin** de un monedero a otro es un proceso bastante simple y directo. Esencialmente, se asemeja al proceso de enviar un correo electrónico. Primero, necesitas tener **bitcoin** en tu monedero y acceso a internet. Luego, al abrir tu monedero de **bitcoin**, simplemente introduces la **dirección** del monedero del destinatario, la cantidad de **bitcoin** que deseas enviar (que debe ser igual o menor al total de **bitcoin** que tienes) y pulsas el botón de envío. Aunque todos pueden ver los detalles de la **transacción** en la **blockchain**, las identidades reales de las partes involucradas permanecen en el pseudo-anonimato. Esto se debe a que las **direcciones** de **bitcoin** no están vinculadas directamente a la identidad personal de los usuarios, ofreciendo así un nivel de privacidad.



### 5.1.7 Si enviar bitcoin es tan sencillo como enviar un correo electrónico, ¿qué me impide duplicar el mismo bitcoin y enviarlo a varias personas?

Podrías pensar que en el mundo digital es fácil hacer copias de algo, como un **bitcoin**, y enviarlo a varias personas. Pero en el universo de **Bitcoin**, esto se evita gracias a una solución efectiva para el problema del "doble gasto".

No hay una única entidad, como un banco, que verifique todas las **transacciones** de **Bitcoin**. En su lugar, hay una red global de nodos, que son básicamente computadoras, encargadas de asegurarse de que cada **bitcoin** se gaste de forma correcta y única. Cuando realizas una **transacción**, esta se difunde a toda esta red de nodos. Cada nodo revisa que realmente eres el dueño del **bitcoin** que estás intentando gastar y, crucialmente, que no lo has gastado antes.



# El Futuro del Dinero Sólido: Introducción al Bitcoin

Puedes imaginarte esta red como un libro de registros colectivo que se va actualizando constantemente y que todo el mundo puede revisar. Si tratas de gastar un **bitcoin** más de una vez, la red lo detectará. Cada **transacción** crea un nuevo registro que se añade de forma irreversible al libro. De esta manera, el sistema de **Bitcoin** se mantiene transparente y seguro, asegurando que cada **bitcoin** solo se pueda gastar una vez.



La “**cadena de tiempo**” o “**timechain**” actúa como este libro inmutable que registra cada **transacción** en orden secuencial. Es transparente para todos, pero a la vez seguro y no puede ser alterado sin el acuerdo de la comunidad. Así es cómo **Bitcoin** mantiene la integridad de todo el sistema. En **Bitcoin**, la “**timechain**” es esencialmente la “**blockchain**” con un énfasis en la cronología y el tiempo que lleva minar y agregar nuevos bloques. (Usaremos el término **blockchain** para referirnos al **timechain** de **BTC**)

## 5.1.8 ¿Cómo ingresan nuevos bitcoins a la red?

Piensa en **bitcoin** como oro digital. Aunque hay un límite máximo de 21 millones de **bitcoins** que pueden existir, no todos están disponibles desde el inicio. Se van “descubriendo” mediante un proceso llamado minería. Pero en lugar de excavar en la tierra como con el oro, los mineros de **Bitcoin** usan computadoras para participar en una especie de lotería matemática.

Cuando ganan esta “lotería”, reciben nuevos **bitcoins** como premio. Esto es su recompensa por mantener el sistema protegido contra actividades fraudulentas y asegurar que cada **bitcoin** se use correctamente. Entonces, aunque pueda parecer misterioso, cada nuevo **bitcoin** es básicamente un premio por el esfuerzo de los mineros.

## 5.1.9 ¿Se puede apagar o prohibir Bitcoin?

No se puede “apagar” o “prohibir” completamente **Bitcoin** debido a su naturaleza descentralizada. Mientras haya interés en su uso, **Bitcoin** seguirá existiendo y funcionando. A continuación, las razones principales:

- **Red Global Descentralizada:** **Bitcoin** funciona en una red global de computadoras. Sin un punto central, no hay una manera de apagarlo completamente.
- **Independencia de Control:** Nadie es el jefe de **Bitcoin**. Ni una sola persona o gobierno lo controla. Cualquiera puede usarlo descargando el software (acceso a monedero digital), lo cual permite enviar y recibir **bitcoins**.
- **Herramientas de Evasión:** A pesar de las restricciones gubernamentales, herramientas como las VPN permiten a los usuarios eludir bloqueos y seguir accediendo a **Bitcoin**.
- **Naturaleza Intangible:** A diferencia de activos físicos como el oro, **bitcoin** es digital, lo que complica su rastreo y confiscación.
- **Alternativas Centralizadas:** Aunque algunos países han creado monedas digitales propias, estas son centralizadas y no brindan las libertades inherentes a **bitcoin**. Es por esto que muchos siguen prefiriendo **bitcoin** sobre estas alternativas.



## Capítulo #5

### 5.2 ¿Quiénes son los Protagonistas en el Mundo de Bitcoin? Los Roles Clave en la Red.

En la **red Bitcoin**, hay tres tipos principales de participantes:

- **Mineros** son computadoras en la **red de Bitcoin** que escriben y verifican nuevas **transacciones** en la **blockchain** añadiendo nuevos bloques a ella. ¡Los mineros son recompensados con **bitcoin** por el trabajo que realizan!
- **Nodos** son computadoras en la **red de Bitcoin** que rechazan, validan y almacenan **transacciones** y bloques. Los nodos no reciben recompensa por su trabajo.
- **Desarrolladores** son responsables de mantener y proponer mejoras al software de **Bitcoin** (es decir, su código computacional). Aseguran que cada computadora en la red siga las reglas y funcione correctamente.

En general, estos tres grupos trabajan juntos para mantener en funcionamiento la **red de Bitcoin** y garantizar que siga siendo segura y descentralizada. También podríamos considerar los siguientes participantes secundarios:

- **Usuarios** son personas comunes que usan **bitcoin**. Envían y reciben **bitcoin** a través de sus monederos y también pueden hacer compras o intercambiarlo por otras monedas.
- **Exchanges** o plataformas de intercambio permiten a los usuarios comprar, vender e intercambiar **bitcoin**, y facilitan **transacciones** en la red. Sin embargo, estas plataformas no desempeñan un papel directo en la operación de la **red de Bitcoin** en sí misma.

Para entender mejor, la **red de Bitcoin** puede compararse con un **sistema de transporte**:

- **Los Mineros de Bitcoin** son como los operadores de estaciones de peaje en una autopista de alta tecnología.

Cada vehículo (**transacción** de **bitcoin**) que pasa por la estación de peaje debe ser registrado y verificado por estos operadores. Se aseguran de que cada vehículo tenga sus papeles en regla, como si comprobaran que la matrícula es válida y que no hay señales de actividad sospechosa, como un robo de vehículo.



Por este servicio esencial de "verificación y registro," los operadores de peaje (mineros) son recompensados con "**cupones de combustible**". Este incentivo los motiva a mantenerse vigilantes, asegurando que solo los vehículos legítimos pasen a través del peaje, lo que contribuye a la seguridad y fluidez del tráfico en toda la "**autopista de Bitcoin**".



Estas intersecciones o peajes mantienen un registro del tráfico que ha pasado, muy parecido a cómo los nodos mantienen un registro de todas las **transacciones** que han ocurrido.

# El Futuro del Dinero Sólido: Introducción al Bitcoin

- **Los Nodos:** se pueden comparar con áreas de servicio a lo largo de las carreteras.

Al igual que una área de servicio es un lugar para detenerse, comer algo, o usar los baños, un nodo en la red de **blockchain** es un punto donde las **transacciones** son procesadas, validadas y almacenadas.

De la misma forma en que las áreas de servicio tienen zonas de descanso y aparcamientos, los nodos disponen de sus propias salas de espera (mempool) donde las **transacciones** verificadas "descansan" antes de continuar su camino hacia la **blockchain**.

Las áreas de servicio no cobran por tu estancia o uso del lugar, de la misma manera los nodos no cobran por almacenar y validar las **transacciones**.



- **Desarrolladores:** son como los ingenieros que diseñan, construyen y mantienen el sistema de autopistas.

Imagina un sistema de autopistas donde cualquier ingeniero calificado pueda proponer mejoras o reparaciones. Los desarrolladores de **Bitcoin** priorizan la seguridad sobre todo, incluso si eso significa que las mejoras toman más tiempo en implementarse. Antes de construir un nuevo carril o cambiar una señal de tráfico, los ingenieros (desarrolladores) revisan detenidamente los planos y realizan pruebas de seguridad.



- Los **usuarios** de la autopista pueden dar su opinión sobre las nuevas construcciones o reparaciones, asegurando que las carreteras satisfagan las necesidades de la mayoría.

- Un **monedero de Bitcoin** es similar a un garaje para tu vehículo.

De la misma manera que un garaje es un lugar seguro para guardar tu carro cuando no está en uso, un **monedero de Bitcoin** es un lugar seguro para guardar tus **bitcoins**.



- Las casas de cambio o **intercambios** son similares a los concesionarios de autos.

Tal como un concesionario te permite comprar y vender carros, una casa de cambio te permite comprar y vender **bitcoin**.

Supongamos que tienes un carro (un **bitcoin**) y quieres mantenerlo seguro cuando no lo conduces. Puedes meterlo en tu garaje (un monedero **bitcoin**) y **cerrar** la puerta (bloquear tu monedero con una **clave**). Esto protegerá tu carro (**bitcoin**) de los ladrones (hackers). Cuando quieras utilizar tu carro (gastar tu **bitcoin**), puedes **abrir** la puerta del garaje y desbloquear tu monedero con otra **clave**, que es necesaria para encender el carro y sacarlo del garaje (hacer una **transacción**).





## Capítulo #5

Considera a **Bitcoin** en términos de un viaje en carro:

Empiezas tu viaje en tu garaje personal (tu monedero de **Bitcoin**) con un carro valioso que deseas vender: un **bitcoin**. Tu objetivo es viajar por una "autopista digital" (la **red de Bitcoin**) para llegar a un concesionario (plataforma de intercambio), donde puedes encontrar un comprador para tu carro (**bitcoin**).



En tu ruta, te detienes en estaciones de servicio (nodos de la red). En cada estación, los operadores comprobaran que tu carro (la **transacción** de **bitcoin**) está en buenas condiciones y sigue las normas de la autopista (la **red de Bitcoin**).

Luego, atravesas peajes (mineros) que registran tu paso y confirman la legitimidad de tu **transacción** en sus libros de registros (bloques). Aquí se verifica a fondo tu **transacción**, asegurándose que todo está en su lugar.

Durante todo el viaje, aprecias que la autopista está constantemente en mantenimiento y mejora por un equipo de ingenieros dedicados (los desarrolladores de **Bitcoin**). Estos profesionales trabajan incansablemente para actualizar y mejorar el sistema de **Bitcoin**, haciendo que esta autopista digital sea cada vez más eficiente y segura para tu viaje.

Finalmente, llegas al concesionario (la plataforma de intercambio), donde se completa la venta de tu carro. Recibes el pago en dinero tradicional y el concesionario se encarga de la transferencia del **bitcoin** al comprador.

En retrospectiva, **Bitcoin** es como un vehículo avanzado que nos permite alcanzar destinos financieros que antes eran inaccesibles con los sistemas financieros tradicionales. Al proporcionarnos la capacidad de realizar **transacciones** y almacenar valor de maneras novedosas, **Bitcoin** ha revolucionado nuestra comprensión del dinero y ha allanado el camino hacia un futuro financiero más abierto, transparente y descentralizado.

### 5.3 Cómo Funciona una Transacción de bitcoin en Bitcoin

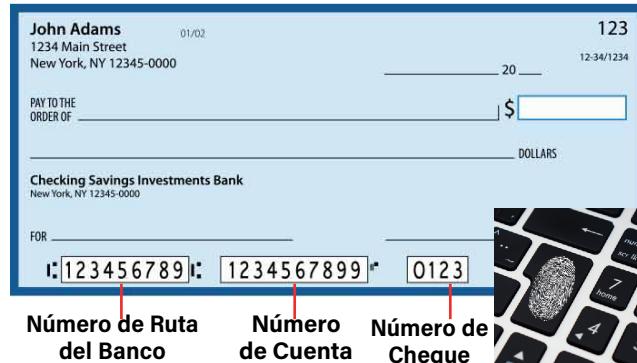
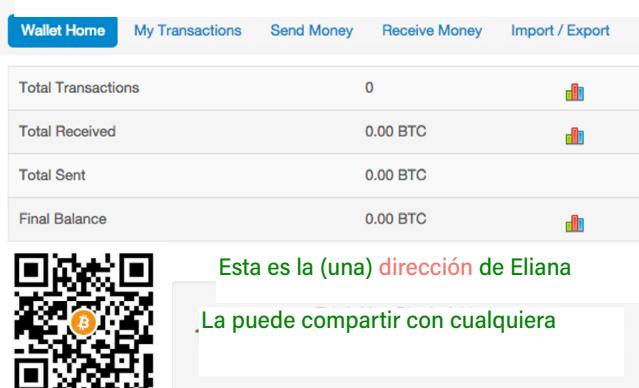
Las **transacciones** de **bitcoin** funcionan de manera distinta al sistema bancario tradicional. En lugar de usar un banco para manejar y confirmar **transacciones**, **Bitcoin** emplea su propia red y un registro de "**cadena de tiempo**". No estamos hablando de mover monedas físicas de un lugar a otro; lo que realmente ocurre son intercambios digitales de valor. Estos se comprueban y se guardan de forma segura en un libro contable abierto y compartido, todo en un orden secuencial. Ahora, veamos cómo funciona esto con más detalle:

**Inicio de la transacción:** Supongamos que Jim le va a pagar 0.5 **BTC** a Eliana. Ambos tienen monederos digitales en sus dispositivos móviles, los cuales pueden abrir como cualquier otra aplicación para ver su saldo de **bitcoins**. Eliana comparte su **dirección** de monedero con Jim, que es similar a un número de cuenta bancaria.

# El Futuro del Dinero Sólido: Introducción al Bitcoin

**Entrada de detalles de la transacción:** Jim ingresa en su monedero la **dirección** de Eliana y la cantidad de **bitcoins** que desea transferir (0.5 **BTC**). Esta etapa es similar a llenar un formulario de transferencia bancaria o escribir un cheque.

## |El Monedero de Eliana-Es su propio banco



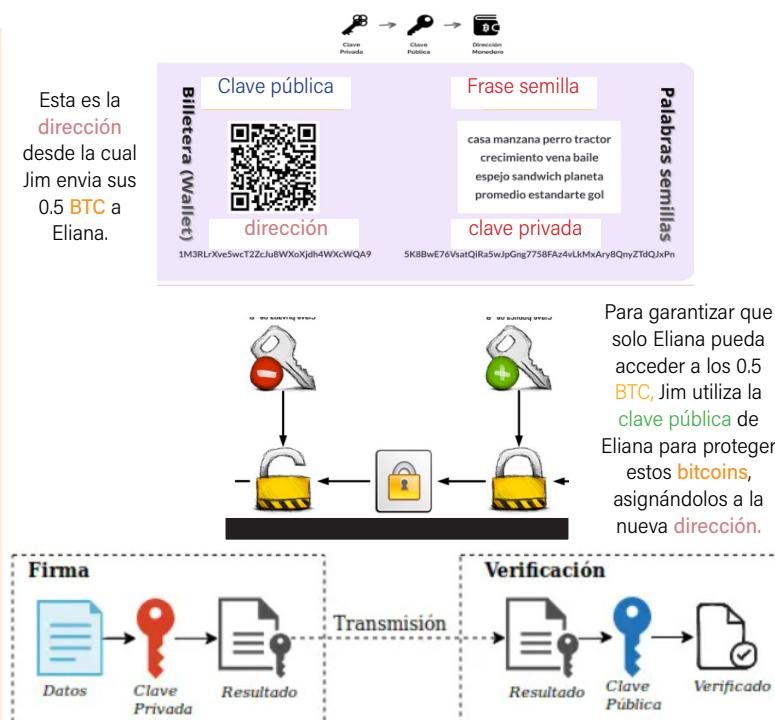
**Firma de la transacción:** Para garantizar la autenticidad de la **transacción**, Jim utiliza su **clave privada** para **firmar** digitalmente la **transacción**. Una **clave privada** en una **transacción de Bitcoin** puede compararse con una firma manuscrita única en un cheque o contrato autenticado en el mundo físico. Así como tu firma manuscrita valida y autoriza la transferencia de fondos o la aceptación de un acuerdo, la **clave privada** en el mundo de **Bitcoin** se utiliza para **"autorizar"** **digitalmente** las **transacciones** y demostrar que eres el legítimo propietario de los **bitcoins** que deseas gastar. Sin embargo, a diferencia de una firma manuscrita que es visible para todos, la **clave privada** permanece secreta y nunca se revela durante la **transacción**. Solo el resultado de la **firma digital** se muestra en la red.



Al hacer clic en "**enviar**", el monedero de Jim utiliza su **clave privada** para desbloquear 0.5 **BTC** y así "**firmar**" la **transacción**, sin revelar su **clave privada**.

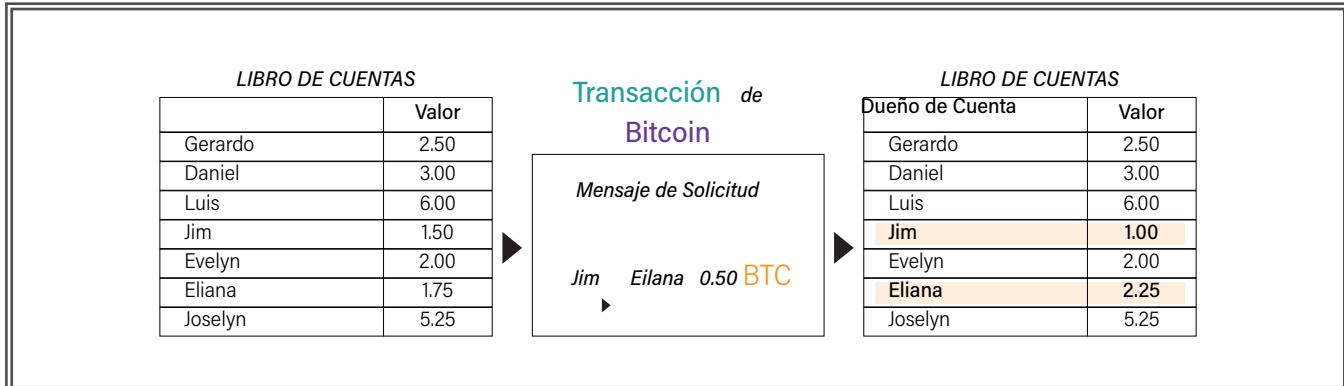
De esta manera, Jim **informa a la red** que "**soy el propietario de esta cuenta y apruebo la transferencia de 0.5 bitcoins a la cuenta de Eliana**".

Además, como parte de esta **transacción**, los 0.5 **BTC** que se envían a Eliana se protegen con su **clave pública**, asegurando que solo ella pueda acceder a esos fondos en el futuro utilizando su **clave privada** correspondiente.





## Capítulo #5



**Verificación de la firma:** Cuando un usuario como Jim **firma** digitalmente una **transacción** con su **clave privada** y la envía a la red, los nodos utilizan su **clave pública** para verificar que la **transacción** haya sido efectivamente firmada por él. Este proceso asegura que la **transacción** es legítima y que fue iniciada por el propietario real de los **bitcoins**.

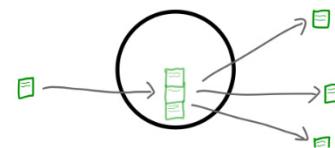
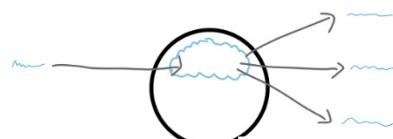
**Verificación de la transacción:** Además de verificar la **firma**, los nodos también comprueban que los **bitcoins** que se van a transferir realmente existen y no se han gastado anteriormente. Esto se hace consultando el historial de **transacciones** almacenado en la **blockchain**.



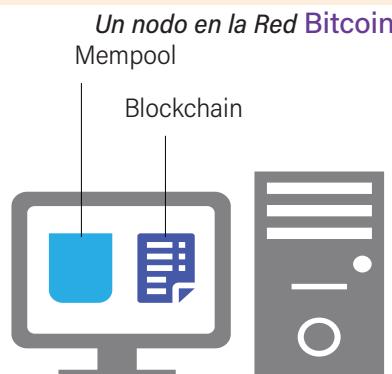
La **mempool**, o "piscina de **transacciones**", es una lista que contiene todas las **transacciones** válidas que aún no han sido incluidas en la **cadena de bloques** de **Bitcoin**. Esta lista se encuentra en un área de almacenamiento de memoria en cada nodo de la red. Cada vez que se crea una **transacción válida**, se agrega a la mempool y espera su inclusión en un bloque.

**Validación de la transacción:** Cuando la mayoría de los nodos confirman que la **transacción** es válida y que Jim dispone de los fondos necesarios, la **transacción** se reconoce como legítima. Luego, se almacena temporalmente en una zona de cada nodo llamada 'mempool'. Aquí permanece la **transacción** hasta que algún minero la incluya en un próximo bloque.

Los nodos comparten **transacciones** frescas



Los nodos comparten bloques enteros de **transacciones** confirmadas



# El Futuro del Dinero Sólido: Introducción al Bitcoin



Una vez verificadas las **transacciones**, deben registrarse permanentemente en la **blockchain**. Un grupo de nodos llamados “**mineros**” compiten por ser los primeros en añadirlas a la **blockchain** y recibir una recompensa por actuar como intermediarios.

**Minería y confirmación:** Imagina la minería de **Bitcoin** como un concurso para resolver un rompecabezas difícil. Los mineros compiten para encontrar la pieza que falta. Quien la encuentra primero, gana el derecho de añadir un **bloque** nuevo al **libro de registros**, que es la **blockchain**. Este bloque recién formado incluye todas las **transacciones** recientes, como la de Jim y Eliana. Una vez que esta pieza se coloca correctamente, el rompecabezas queda sellado y ya no se puede modificar.

Resolver el rompecabezas no es fácil y necesita mucha potencia de computadora. Este esfuerzo asegura que los mineros se tomen en serio su trabajo de validar **transacciones** y de mantener la red segura.

En **Bitcoin**, no hay un pequeño grupo de personas tomando todas las decisiones. La minería actúa como un sistema de control para confirmar **transacciones** y mantener la red operativa.

**Finalización de la transacción:** Finalización de la **transacción**: Una vez que las **transacciones** son incluidas en un bloque y añadidas a la **blockchain**, los **bitcoins** “se consideran transferidos de Jim a Eliana” de manera segura, permanente e irreversible. Eliana puede ahora acceder a los **bitcoins** recibidos.

Es importante recordar que, dado el carácter irreversible de las **transacciones** de **Bitcoin** y la asociación de los **bitcoins** con la **clave privada**, mantener esta clave segura es crucial. Si se pierde, no hay manera de recuperar los **bitcoins** asociados a ella.

Minero



Mueve  
**transacciones**  
válidas a la  
mempool.

Bloque

Piscina de  
**Transacciones**  
/ Mempool



Selección  
**transacciones**  
de mempool y  
Crea el bloque.

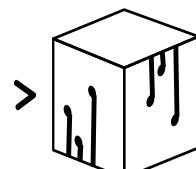
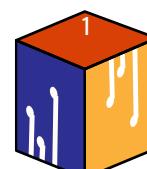


Ejemplo de una **Transacción** en una  
Cadena de Bloques

Jim le pagó a Eliana  
0.50 **BTC** el viernes  
pasado  
x1000

En los días  
siguientes, Eliana le  
pagó a Luis el total  
de 0.637 **BTC**

Luis le pagó a  
Quentin 1.876 **BTC**



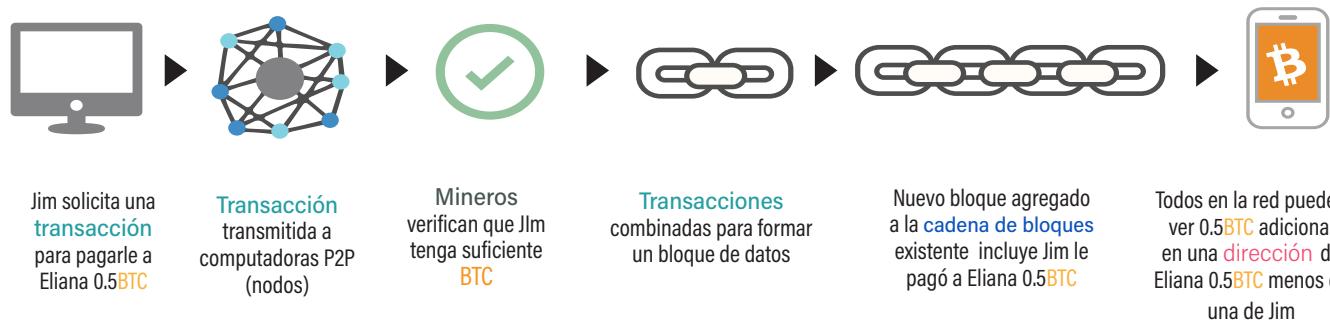
Data  
—  
Orden de las  
**transacciones**





## Capítulo #5

### Cómo Funciona una **Transacción** de Bitcoin



#### 5.3.1 Actividad. Experimentando las **Transacciones** en Acción

*Comprende tu rol.* Se te ha asignado uno de los siguientes roles: remitente, receptor, nodo o minero.

- Los **remitentes** serán responsables de crear y transmitir **transacciones**.
- Los **receptores** serán responsables de recibir y verificar **transacciones**.
- Los **nodos** serán responsables de validar las **transacciones** verificando que la **transacción** sea válida \*\*\*Lo harán verificando las reglas del protocolo y del mecanismo de consenso.
- Los **mineros** serán responsables de agregar las **transacciones** a la **blockchain**.

**1. Como remitente:** Crea una **transacción** siguiendo estos pasos:

- Escribe en una nota de **transacción** la cantidad de monedas que deseas enviar y el nombre o iniciales del receptor.
- Firma** la nota con tu nombre o iniciales, simulando una **clave privada**.
- Pasa la nota de **transacción** y la cantidad correspondiente de **monedas** al receptor.

*Tanto los nodos como los receptores deben verificar las **transacciones**:*

**2. Como receptor:** Eres responsable de verificar las **transacciones**. Sigue estos pasos:

- Verifica la nota de **transacción** para asegurarte de que se haya escrito la cantidad correcta de monedas y el nombre o iniciales del receptor.
- Cuenta las monedas recibidas y compáralas con la cantidad de monedas escrita en la nota.
- Si las monedas coinciden, marca la casilla de aprobación.
- Si las monedas no coinciden o tienes dudas, rechaza la **transacción**.

# El Futuro del Dinero Sólido: Introducción al Bitcoin

Moneda Enviada	Remitente	Firma del Remitente	Receptor	Fecha y Hora	Aprobación del Receptor

**3. Como nodo:** Verifica y valida las **transacciones**. Eres responsable de verificar que la **transacción** sea válida.

- Verifica que la **dirección** del remitente sea válida y que la **dirección** del receptor sea válida.
- Comprueba que el remitente tenga suficientes fondos para completar la **transacción** y que la **transacción** no duplique el gasto de ninguna moneda.

**4. Como minero:** Agrega **transacciones a la blockchain**. Eres responsable de agregar las **transacciones** a la **blockchain**.

- Verifica las **transacciones** que han sido aprobadas por los receptores y validadas por los nodos.
- Encuentra la pieza del rompecabezas que falta.
- El primero encuentre la pieza del rompecabezas agregará la **transacción** a la **blockchain**.
- Una vez que se agrega una **transacción** a la **blockchain**, no se puede cambiar ni revertir.

**5. Realiza un seguimiento de tu saldo de monedas:** A lo largo de la actividad, realiza un seguimiento de tu saldo de monedas contando las monedas en tu monedero digital.

## 5.4 Un Nuevo Enfoque hacia el Dinero

**Bitcoin** no nació solo como una nueva tecnología. Fue diseñado para abordar problemas reales que la gente enfrenta cada día, especialmente después de la crisis financiera de 2008. La idea era simple pero poderosa: crear un sistema financiero que fuera abierto, seguro y que pusiera el control en manos de las personas, no de grandes instituciones.

**Bitcoin** ofrece algo más que solo una forma de pagar cosas. Ofrece una nueva forma de pensar sobre lo que es el dinero. Permite a las personas tomar el control de su riqueza y tener más seguridad en cómo la guardan y gastan. Y todo esto se hace con un uso de energía y una seguridad en las **transacciones** que desafían los métodos tradicionales.

Así que **bitcoin** no es solo un nuevo tipo de dinero. Es una revolución que nos permite imaginar un mundo donde el poder financiero está más repartido. Y esto es solo el comienzo.



## Capítulo #5

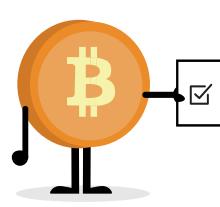
### 5.4.1 ¿Cuál es la mayor diferencia entre Bitcoin y la banca tradicional?

**Bitcoin**, desde su inicio en 2009, ha demostrado ser una alternativa innovadora y robusta a los sistemas financieros tradicionales. Aquí están sus ventajas clave:

- **Descentralización:** A diferencia de los bancos, **Bitcoin** opera sin un servidor central que controle la red, lo que significa que no está sujeto a las políticas y decisiones de una entidad en particular.
- **Accesibilidad:** **Bitcoin** es accesible para cualquier persona con una conexión a Internet, lo que puede ayudar a abordar la desigualdad de riqueza.
- **Transparencia y seguridad:** Todas las **transacciones** de **bitcoin** son públicas y verificables, pero a la vez **pseudónimas**. Aunque los nombres no se muestran, hay números y códigos que representan a las personas. Es un sistema en el que hay reglas claras para todos, pero no hay una persona o entidad controlándolo todo. Es como un juego justo donde todos conocen las reglas, pero no hay un árbitro que pueda cambiarlas a mitad del juego.
- **Suministro limitado:** El protocolo de **Bitcoin** establece un límite de **21 millones** de **bitcoins**, lo que podría ayudar a preservar su valor a largo plazo.
- **Transacciones internacionales eficientes:** **Bitcoin** permite **transacciones** internacionales rápidas y a menudo más económicas en comparación con las transferencias bancarias tradicionales.



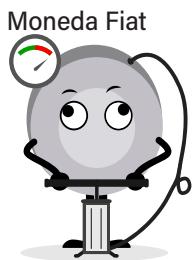
Inflación controlada, cantidad en circulación predecible y predefinida.



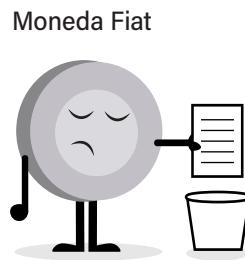
Sólo se pueden aplicar cambios si los usuarios los aceptan.



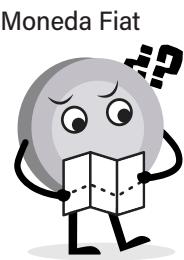
No tienen fronteras, puede ser aceptada por cualquier persona en el mundo.



Inflación a niveles récord y puede ser devaluada cuando se imprime sin control.



Cambia a gusto de los mandatarios y sin consultar a los ciudadanos.



Sólo es aceptado dentro del país y no puede usarse fuera del país.

# El Futuro del Dinero Sólido: Introducción al Bitcoin

## 5.4.2 Evaluando el Consumo Energético: Bitcoin frente a la Banca y la Minería Tradicionales

### Consumo Energético de Bitcoin: Hechos y Contexto

La minería de **bitcoin** utiliza aproximadamente 70 teravatios-hora al año. Sin embargo, es importante entender que esta cifra no debe tomarse de manera aislada. La minería de **bitcoin** tiene el potencial de aprovechar energías renovables y contribuir a la investigación y desarrollo de energías más limpias.

### Energía Monetaria: Inversión Inicial y Eficiencia

En la minería de oro y en la minería de Bitcoin, se requiere una inversión inicial considerable en maquinaria y equipo especializado. Sin embargo, la eficiencia en la minería de Bitcoin está determinada por la potencia de los ASICs, mientras que en la minería de oro, la eficiencia depende del tipo de maquinaria física utilizada. Este aspecto resalta cómo la minería de Bitcoin tiene el potencial de ser más eficiente en términos de retorno de la inversión y uso de recursos.

### El Sistema Financiero Tradicional

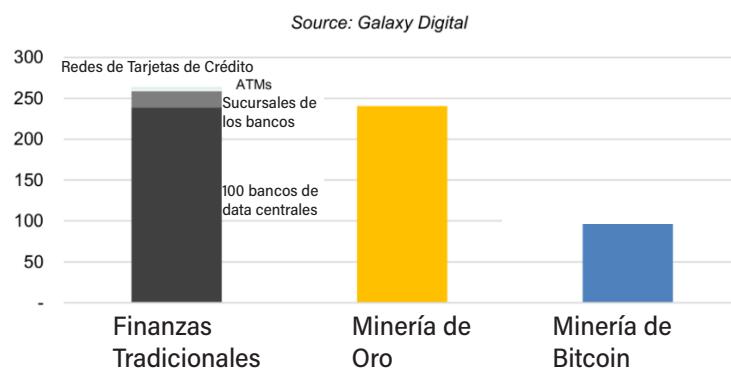
Los bancos, cajeros automáticos y la infraestructura que respalda las monedas tradicionales también consumen energía, y de hecho, pueden llegar a ser menos eficientes que Bitcoin en términos energéticos. Aunque no hay una cifra exacta, se estima que el sistema financiero global podría utilizar mucho más que los 95 teravatios-hora anuales consumidos por la minería de Bitcoin.

### Minería de Oro: Otro Consumidor Energético

La minería de oro no solo consume una cantidad significativa de energía sino que también tiene un impacto ambiental en términos de desforestación y uso de productos químicos tóxicos. A diferencia de Bitcoin, la minería de oro tiene un historial de prácticas laborales cuestionables y daño ambiental irreparable.

Estimado Actual de Consumo Energético (TWh/año)

fuente: Galaxy Digital



Al considerar todo el panorama, el consumo energético de Bitcoin no es necesariamente más dañino que el de otras industrias y sistemas financieros. Además, hay un creciente interés en la adopción de energías renovables en la minería de Bitcoin, lo cual puede reducir aún más su impacto ambiental en el futuro.



## Chapter #5

### 5.5 ¿Son seguras las transacciones con bitcoin?

La criptografía es una característica distintiva de **Bitcoin** en comparación con los sistemas bancarios tradicionales. Mientras que en la banca las **transacciones** son validadas por intermediarios como los bancos, en la **blockchain** de **Bitcoin**, las **transacciones** son autenticadas por miles de computadores mediante criptografía.

¿Qué es la criptografía?



La **criptografía** es como un código secreto que solo tú y el receptor pueden descifrar. Es una forma de mantener la información en secreto al disfrazarla en un código. Es una técnica que protege la comunicación, manteniendo los datos seguros y permitiendo que solo las personas autorizadas puedan acceder a ellos.

La **encriptación** es el proceso de convertir información en un código especial, de tal manera que se vuelve ilegible para cualquiera que no tenga el método correcto para descifrarlo. Esto es similar a **cerrar** una caja fuerte, donde solo la persona con la llave o combinación correcta puede abrirla.

Por otro lado, el **descifrado** es el proceso de convertir la información codificada de vuelta a un formato legible, como si estuvieras **abriendo** la caja fuerte y pudiendo leer la información que hay dentro.

Los detalles de una **transacción** en **Bitcoin**, tales como las **direcciones** del emisor y del receptor, así como la cantidad de dinero transferida, son visibles al público a través de la **cadena de bloques**. Sin embargo, la propiedad de los **bitcoins** que se transfieren se verifica mediante el uso de criptografía.

Hagamos de cuenta que Napo y Reyna quieren enviarse un mensaje sin que Ale se entere. Deciden cambiar cada letra del mensaje por la siguiente del abecedario, volviendo el mensaje ininteligible para Ale. Aunque este método ya no es seguro hoy, nos da una idea de lo que es la criptografía "tradicional".

En el universo **Bitcoin**, Napo y Reyna tienen cada uno una **clave pública** y una **privada**. Napo puede cifrar su mensaje usando la **clave pública** de Reyna y enviárselo. Al recibirla, Reyna puede descifrar el mensaje con su **clave privada**. Si Ale logra interceptar el mensaje, no podrá leerlo porque no tiene la **clave privada** de Reyna.

Además, Napo puede **firmar** su mensaje usando **su propia clave privada** para generar una **firma digital**. Al recibir el mensaje, Reyna puede usar la **clave pública** de Napo para **verificar** la **firma** y confirmar que Napo es realmente el remitente.

Veamos un ejemplo simple:

#### Como Resolver este Cifrado

Al resolver el Cifrado Pocilga, el jugador recibe un mensaje grabado y un grabado. Para descifrar el mensaje, el encontrará el símbolo del mensajero reproductor activado en el activado para encontrar la letra descifrada.

\*Ejemplo de un mensaje encriptado:



A	B	C	J	K	L	S	T	U	W	X	Y	Z
D	E	F	M	N	O	X	V					
G	H	I	P	Q	R							



# Capítulo #6

## Desbloqueadas: Navegando la Auto-Custodia y la Red Lightning

- 6.0 De Novato a Experto: Navegando el Mundo de las Carteras de Bitcoin
- 6.1 Rampas de Acceso y Protección de tu bitcoin
  - 6.1.1 Ejercicio de Clase: Dominando la Autocustodia y Usando Monederos con Confianza
- 6.2 On-Chain (Transacciones en Cadena) vs. Off-Chain (Transacciones Fuera de Cadena)
  - 6.2.1 Una analogía de una Transacción On-chain
  - 6.2.2 ¿Cómo Recibo bitcoin on-chain?
  - 6.2.3 Ejercicio de Clase: Cómo Enviar bitcoin y Pagar Bienes y Servicios
- 6.3 La Red Lightning- Una Solución para Transacciones Rápidas y Seguras
  - 6.3.1 Monederos de la Red Lightning
  - 6.3.2 Una Transacción en la Red Lightning
  - 6.3.3 Actividad. Carrera de Relevos de Billeteras Lightning
  - 6.3.4 Ejercicio de Clase: Demo Interactivo en línea de Lightning

# Carteras de Bitcoin Desbloqueadas

## 6.0 De Novato a Experto: Navegando el Mundo de las Carteras de Bitcoin

Un monedero de **Bitcoin**, también denominado "cartera", "billetera" o "wallet", funciona como tu cuenta personal en el universo del **Bitcoin**, donde se almacenan tus **satoshis** (o "sats"). Pero a diferencia de las cuentas bancarias tradicionales que dependen de instituciones financieras como intermediarios, un monedero de **Bitcoin** funciona en una red descentralizada y peer-to-peer, favoreciendo la autonomía y el control directo sobre tus fondos.



Tus **sats** **no** se almacenan realmente en el monedero, ya que el **bitcoin** nunca deja la **cadena de bloques**. En lugar de eso, el monedero almacena un par de claves: una **clave pública** que se puede compartir con otras personas para recibir fondos, y una **clave privada** que se usa para firmar **transacciones**. El propietario de la **clave privada** es el único que tiene acceso a los fondos de **bitcoin** en una cartera específica. (\*Vamos a usar clave y llave intercambiablemente)

Una característica importante de las carteras de **Bitcoin** es la "frase semilla" o "frase de recuperación". Esta es un conjunto único de palabras que se utiliza para generar las **claves privadas** asociadas a tu cartera. Si pierdes el acceso a tu cartera o necesitas restaurarla en otro dispositivo, puedes utilizar la frase semilla para recuperar tus fondos. En este sentido, la frase semilla actúa como una copia de seguridad de tus **claves privadas**, garantizando que puedas acceder a tus **bitcoin** cuando lo necesites.

En el mundo de **Bitcoin**, una **clave privada** es como la llave maestra de tu dinero: te permite acceder y gastar tus fondos. Por otro lado, las **claves públicas** (y las **direcciones** que se generan a partir de ellas) actúan como tu **dirección** de correo: otros pueden verla y enviarte dinero a ella, pero no pueden acceder a tus fondos solo con conocerla.

Existen dos enfoques principales en la generación de claves en los monederos de **bitcoin**:

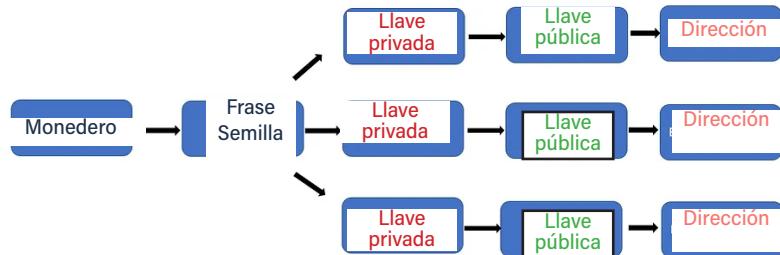
**Monederos de Clave Única:** Estos monederos generan una única **clave privada** y, a partir de ella, generan una **clave pública** y, consecuentemente, una **dirección** de **Bitcoin**. Cada vez que necesitas una nueva **dirección**, el monedero genera una nueva **clave privada**.

**Monederos Determinísticos o HD** (por sus siglas en inglés "Hierarchical Deterministic"): Estos monederos utilizan una "**semilla**" única (un conjunto de palabras) para generar múltiples pares de **claves públicas** y privadas. Esto facilita la administración y el respaldo del monedero. Con solo recordar o guardar de manera segura la semilla, puedes recuperar todas tus **direcciones** y fondos.



# Capítulo #6

A la derecha se muestra cómo una semilla genera múltiples **claves privadas** y cómo cada **clave privada** genera una **clave pública** y **dirección** correspondiente.



## Monederos Custodiales vs No Custodiales

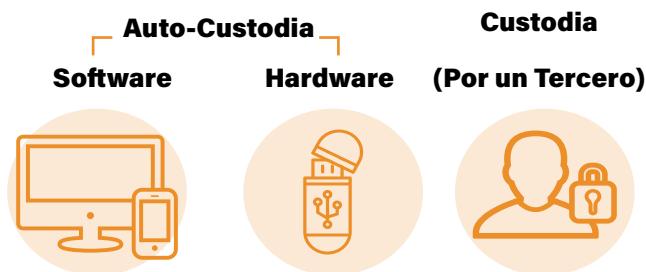
Existen dos tipos principales de monederos de Bitcoin: auto-custodia y custodia. En un monedero de auto-custodia, eres el único poseedor de las claves y tienes control total sobre lo que entra y sale. En un monedero de custodia, una tercera parte tiene la clave y puede acceder y administrar el contenido de la cartera en tu nombre. Mientras que la auto-custodia es como ser tu propio banco, proporcionando mayor privacidad y control, también significa que asumes la plena responsabilidad de mantener seguro tu **bitcoin**.

La diferencia principal entre un monedero (o billetera) de custodiada y un de no custodiada reside en quién tiene el control de las **claves privadas** (que dan acceso a tus **bitcoin**):

En una billetera **no custodiada**, tú **controlas las claves privadas**. Esto significa que solo tú puedes mover tus fondos, pero también que eres responsable de su seguridad. Si pierdes tu clave, podrías perder tus fondos para siempre.

En una billetera **custodiada**, una tercera entidad (como un intercambio de criptomonedas) **tiene el control de tus claves**. No necesitas preocuparte por perder tu clave, pero dependes de la tercera entidad para la seguridad de tus fondos.

Aquí unos indicativos adicionales para reconocer cada tipo:



- **Frase de recuperación:** Las billeteras no custodiadas suelen proporcionarte una frase de recuperación que puedes usar para restaurar tus fondos en caso de pérdida.
- **Dependencia del servicio de terceros:** Si necesitas iniciar sesión en una aplicación o sitio web para acceder a tus fondos, probablemente estés usando una billetera custodiada.
- **Privacidad:** Las billeteras custodiadas a menudo requieren información personal debido a regulaciones (KYC, AML), mientras que las billeteras no custodiadas suelen requerir menos información.
- **Transacciones:** Con una billetera no custodiada, puedes realizar **transacciones** de inmediato. En cambio, en una custodiada, la entidad puede necesitar aprobar la **transacción**, lo que podría demorarla.

# Carteras de Bitcoin Desbloqueadas

Tipo de Monedero	Descripción	Ventajas	Desventajas	Tipo de Usuario
Custodiales	Un tercero controla tus <b>claves privadas</b> .	Fáciles de usar, opción de recuperación si pierdes tu contraseña.	Confías en un tercero para la seguridad de tus <b>bitcoins</b> .	Usuarios nuevos o aquellos que no se sienten cómodos manejando sus propias <b>claves privadas</b> .
No Custodiales	Tú tienes el control de tus <b>claves privadas</b> .	Control total sobre tus <b>bitcoins</b> , mayor privacidad.	Responsabilidad total, si pierdes tus claves, pierdes tus <b>bitcoins</b> .	Usuarios con conocimientos técnicos o aquellos que quieren tener el control total sobre sus <b>bitcoins</b> .

Al considerar cómo almacenar tus **bitcoins**, no solo es crucial determinar quién tiene el control de tus **claves privadas**, sino también la conveniencia, el control que deseas tener sobre tus **claves privadas**, y la frecuencia con la que planeas realizar **transacciones**. Independientemente del monedero que elijas, recuerda siempre que la seguridad de tus **bitcoins** depende en gran medida de cómo manejes y protejas tus **claves privadas**.

## Monederos Calientes vs Monederos Fríos

Existen dos tipos de monederos dependiendo de su **conexión a Internet**: Monederos Calientes y Monederos Fríos

Tipo de Monedero	Descripción	Ventajas	Desventajas	Tipo de Usuario
Calientes	Conectados a Internet, fáciles de configurar y usar.	Acceso rápido y fácil a los <b>bitcoins</b> .	Vulnerables a los ataques en línea.	Apropiado para usuarios que realizan <b>transacciones</b> frecuentes y que manejan pequeñas cantidades de <b>Bitcoin</b> .
Fríos	Desconectados de Internet	Proporcionan un nivel de seguridad adicional. Mayor seguridad al estar aislados de Internet.	Menos conveniente para las <b>transacciones</b> diarias.	Apropiado para usuarios que almacenan grandes cantidades de <b>Bitcoin</b> y no realizan <b>transacciones</b> a menudo.

## Tipos de Monederos por Plataforma

Los monederos pueden clasificarse por la plataforma en la que operan: escritorio, móviles, hardware y web.

Tipo de Monedero	Descripción	Ventajas	Desventajas	Tipo de Usuario
Escritorio (Desktop)	Instalados en tu PC o laptop.	Control total sobre tus <b>bitcoins</b> , no requieren confiar en un tercero.	Pueden ser vulnerables si tu PC es hackeada.	Usuarios con un nivel medio de conocimientos técnicos.
Móviles (Software)	Aplicaciones instaladas en tu smartphone.	Convenientes, puedes llevar tus <b>bitcoins</b> donde quiera que vayas.	Pueden ser vulnerables si tu smartphone es hackeado.	Usuarios que desean tener sus <b>bitcoins</b> al alcance de la mano para <b>transacciones</b> rápidas.
Hardware	Monederos físicos que almacenan tus <b>claves privadas</b> fuera de línea.	Seguridad adicional, menos vulnerables a los ataques en línea.	Requieren una inversión inicial, menos convenientes para <b>transacciones</b> diarias.	Usuarios que tienen una cantidad considerable de <b>Bitcoin</b> y quieren la máxima seguridad.
Web	Accesibles a través de un navegador web.	Fáciles de usar, accesibles desde cualquier lugar.	Confías en un tercero para la seguridad de tus <b>bitcoins</b> .	Usuarios nuevos o aquellos que quieren acceso fácil a sus <b>bitcoins</b> .



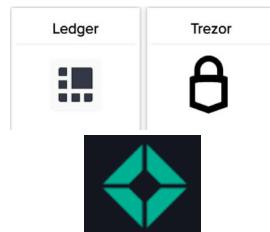
## Capítulo #6

La semi-custodia es un punto medio entre la custodia total y la no custodia. En este sistema, tanto tú como una tercera entidad tienen acceso a tus **claves privadas**. Esto significa que si pierdes tus claves, la tercera entidad podría ayudarte a recuperar tus fondos. Sin embargo, aún mantienes el control principal de tus fondos.

Por ejemplo, algunas billeteras ofrecen una función de recuperación de cuenta. En este caso, la entidad de la billetera tiene una clave de respaldo, pero tú todavía tienes la principal. Aunque este sistema tiene ventajas, debes confiar en que la tercera entidad será honesta y segura.

Recuerda que siempre puedes mover tus fondos a otra billetera si tus necesidades cambian. El tipo de billetera que elijas dependerá de tus circunstancias personales y de tus necesidades.

- 1. Seguridad:** Asegúrate de que el monedero tenga robustas medidas de seguridad como la autenticación de dos factores y políticas de contraseñas robustas.
- 2. Privacidad:** Determina si el monedero protege tu privacidad o si necesitas proporcionar información personal para usarlo.
- 3. Facilidad de Uso:** Si eres nuevo en Bitcoin, opta por un monedero con una interfaz de usuario intuitiva.
- 4. Compatibilidad:** Comprueba que el monedero sea compatible con tu dispositivo y sistema operativo.
- 5. Tarifas:** Revisa y compara las tarifas que aplican diferentes monederos para conseguir el que mejor se adapte a tu presupuesto.
- 6. Reputación:** Haz una investigación sobre la reputación del monedero y su equipo de desarrollo para garantizar su confiabilidad.
- 7. Control:** Decide si prefieres un monedero que te permita un control total de tus **claves privadas** (auto-custodia) o uno que priorice la facilidad de uso, pero con menos control (custodia).



Monederos Hardware



Monederos de Escritorio



Monederos Móvil



Ejemplo de monedero de papel bitcoin creado con bitaddress.org

Monederos de Papel



Monederos Web

# Carteras de Bitcoin Desbloqueadas

## 6.1 Rampas de Acceso y Protección de tu bitcoin

El primer paso es adquirir **bitcoin**, lo cual puedes hacer mediante diversas opciones como casas de cambio, brokers, cajeros automáticos de **Bitcoin** (BTM), compañías fintech, e incluso tarjetas de regalo. Estos servicios, a menudo referidos como “**rampas de acceso**”, te permiten intercambiar dinero convencional, como euros o dólares, por su equivalente en **bitcoin**.

En las siguientes secciones, te proporcionaremos pasos claros y seguros sobre cómo adquirir y proteger tus **bitcoins**.

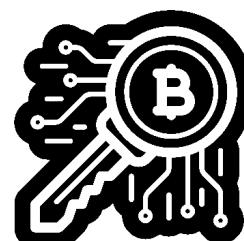
- 1. Elige un exchange o broker de bitcoin:** Existen varias plataformas para comprar y vender **bitcoin**. Elige una que sea de confianza y cumpla con tus necesidades.
- 2. Crea una cuenta:** Sigue las instrucciones de la plataforma para abrir una nueva cuenta. Puede ser necesario proporcionar información personal y verificar tu identidad.
- 3. Conecta un método de pago:** La mayoría de las plataformas te permitirán conectar una cuenta bancaria, tarjeta de crédito o débito para financiar tu cuenta. Sigue las instrucciones para agregar tu método de pago.
- 4. Realiza una orden de compra:** Una vez que tu cuenta esté configurada y financiada, puedes ordenar la compra de **bitcoin**. La plataforma te proporcionará una cotización y podrás especificar la cantidad de **bitcoin** que deseas comprar.
- 5. Confirma la transacción:** Revisa los detalles de tu **transacción** y confirma la compra. La plataforma procesará la **transacción** y el **bitcoin** será transferido a tu cuenta en la plataforma.
- 6. Retira el bitcoin:** Si deseas transferir el **bitcoin** a un monedero auto-custodiado, necesitarás retirar el **bitcoin** de la plataforma y enviarlo a tu monedero. La plataforma proporcionará las instrucciones para hacerlo.



**Importante:** La frase que ves a tu derecha refiere a la idea de que si no tienes control directo sobre las **claves privadas** asociadas con tu monedero de **bitcoin**, no eres el verdadero dueño de las monedas.

La **clave privada** es un código secreto que te permite acceder y gastar tus **bitcoins**. Cuando almacenas tu **bitcoin** con un servicio de terceros, como un exchange o monedero online, dependes de dicho servicio para mantener segura tu **clave privada**. Si el servicio es hackeado o cierra, podrías perder acceso a tus **bitcoins**.

Por lo tanto, es importante que controles tus propias **claves privadas** y las almacenes de manera segura. De esta forma, tendrás control total sobre tus **bitcoins** y podrás acceder a ellos siempre que lo deseas.



**NO SON TUS CLAVES,  
NO SON TUS  
MONEDAS**



## Capítulo #6

### 6.1.1 Ejercicio de Clase: Dominando la Autocustodia y Usando su Monedero con Confianza

*Ejercicio de Clase.*

*Opción 1. Crea una nueva billetera.*

Confirma la frase semilla  
Inserta cada palabra en el orden que se te presentó en la pantalla previa

**Mi Frase de Recuperación**

 Confidencial!!!!

1.	13.
2.	14.
3.	15.
4.	16.
5.	17.
6.	18.
7.	19.
8.	20.
9.	21.
10.	22.
11.	23.
12.	24.

NEED HELP?

- 1. Descargar la aplicación:** Busca y descarga la aplicación de la billetera desde la App Store (iOS) o Google Play Store (Android).
- 2. Configurar la billetera:** Al abrir la aplicación, te pedirá que introduzcas una frase de recuperación de 12 o 24 palabras. Escribe estas palabras y guárdalas en un lugar seguro. Si pierdes esta frase, no podrás recuperar tus bitcoins.
- 3. Verificar la frase de recuperación:** La aplicación te pedirá que ingreses de nuevo las palabras de tu frase de recuperación para confirmar que las has guardado correctamente.
- 4. Establecer una contraseña:** Algunas billeteras te permiten establecer una contraseña adicional para una mayor seguridad. Si es así, establece una contraseña fuerte y guárdala en un lugar seguro.
- 5. Generar la clave privada y la dirección de bitcoin:** Una vez que hayas configurado todo, la billetera generará automáticamente tu **clave privada** y tu primera **dirección de bitcoin**.
- 6. Recibir bitcoins:** Para recibir bitcoins, puedes compartir tu **dirección de bitcoin** con la persona que te los enviará. Si tu billetera no permite comprar bitcoins directamente, tendrás que hacerlo a través de un intercambio y luego transferirlos a tu billetera usando tu **dirección de bitcoin**.

**Opción 2. Restaura una billetera** (tiempo limitado).

Es probable que tu profesor te de una frase semilla de un monedero ajeno.

- 1. Iniciar la aplicación de la cartera:** Cuando inicies tu aplicación de cartera por primera vez, verás tres métodos para crear una cartera. Selecciona [Importar una cartera existente].
- 2. Introducción a la restauración:** Verás una pantalla de introducción. Aquí, selecciona [Restaurar con frase de recuperación].
- 3. Ingresar la frase de recuperación:** Ahora, tendrás que ingresar tu frase de recuperación de 12, 18 o 24 palabras. Asegúrate de introducir cada palabra en el orden correcto.
- 4. Restaurar la cartera:** Una vez que hayas terminado de ingresar tu frase de recuperación, pulsa [Restaurar/Restaurar].
- 5. Importación exitosa:** Si tu cartera ha sido importada exitosamente, verás un mensaje que dice "Importación Exitosa".

**Recuerda:** Esta frase de recuperación es extremadamente importante. Sin ella, perderás acceso a tus bitcoins si alguna vez pierdes acceso a tu cartera. Por lo tanto, asegúrate de anotarla y guardarla en un lugar seguro.

# Carteras de Bitcoin Desbloqueadas

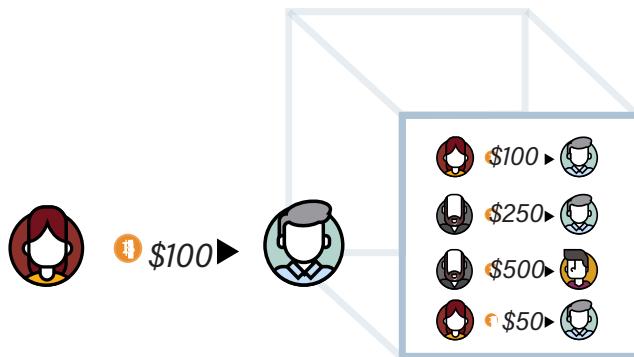
## 6.2 Transacciones en Cadena (On-Chain) vs Transacciones Fuera de Cadena (Off-Chain)

Es importante destacar que no todas las **transacciones** de **bitcoin** se registran en la **blockchain** principal de **Bitcoin**. Algunas se hacen fuera de la cadena para agilizar el proceso y reducir las tarifas. Estas **transacciones** "fuera de la cadena" también son seguras, pero no quedan registradas en el libro público que todos pueden ver.

### Transacciones en Cadena (On-Chain)

1. Son **transacciones** que ocurren directamente en la **blockchain** de **Bitcoin**.
2. Tardan alrededor de 10 minutos en confirmarse y las tarifas dependen del tamaño de la **transacción**.
3. Son seguras y ofrecen la máxima descentralización y resistencia a la censura.

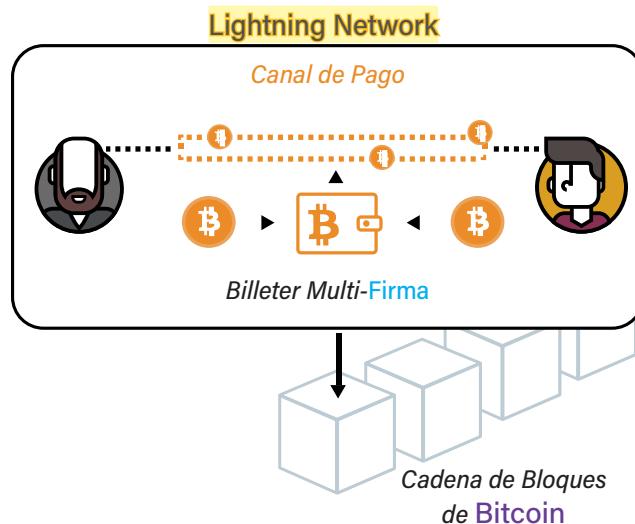
### En la Cadena de Bloques (On Chain)



### Transacciones Fuera de Cadena (Off-Chain)

1. Estas **transacciones** ocurren en una red separada construida sobre la **blockchain** de **Bitcoin**. Esta red se conoce como una "**segunda capa**" que opera sobre la **blockchain**.
2. Se liquidan más rápidamente y con tarifas más bajas.
3. Son comúnmente utilizadas donde las regulaciones y leyes apoyan su adopción y donde la velocidad y el costo de las **transacciones** son más importantes.
4. Aunque la seguridad de las **transacciones off-chain** depende de una serie de factores, la **Red Lightning** está diseñada para ser segura. Las **transacciones** solo se publican en la **blockchain** de **Bitcoin** cuando los canales de pago se abren o cierran.

### Fuera de la Cadena (Off Chain)



# Capítulo #6



## 6.2.1 Una Analogía de una Transacción On-Chain

Visualiza que quieres enviar un mensaje importante a un amigo que vive en otro país. El mensaje sería tu **transacción** de **bitcoin**, y el sobre sellado sería tu monedero de **Bitcoin**. Dentro del sobre, anotas la **dirección** del monedero de tu amigo y la cantidad de **bitcoin** que deseas enviar.

Una vez que el sobre está sellado con tu **firma digital** única (usando tu **clave privada**), lo entregas a un servicio de mensajería global, que representa la **red de Bitcoin**. Este servicio no es operado por una sola empresa, sino por muchas "oficinas" (**nodos**) en todo el mundo.

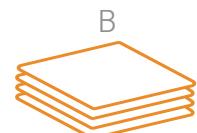
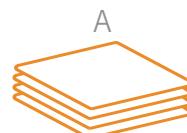
Aquí es donde entra en juego el "**protocolo de seguridad**" del servicio de mensajería (los mineros de **Bitcoin**). Estas reglas verifican automáticamente la autenticidad de tu **firma** y la validez de la información en tu sobre. Es un proceso que requiere tiempo y esfuerzo computacional, pero garantiza que todo sea legítimo. El primer nodo que verifica con éxito tu **transacción** se añade a un conjunto de **transacciones** verificadas (un **bloque**).

Finalmente, este bloque se adjunta a una larga **cadena de bloques** anteriores, formando así la **blockchain**. En el otro extremo, tu amigo recibe el mensaje (los fondos de **bitcoin**) en su monedero personal. No necesita "abrir" el sobre; simplemente, con su propia **clave privada** única, puede acceder a los fondos que le has enviado.

En resumen, a pesar de ser un proceso minucioso y detallado, la **transacción On Chain** resulta ser transparente, segura y confiable, lo que transforma radicalmente la forma en que se realiza la transferencia de valor a nivel global.

La Razón de Ser de la **Firma digital**

Haces una **firma digital** única con tu **clave privada**



La **firma** es una representación digital de los detalles de la **transacción**, incluyendo la cantidad de **bitcoin** que se envía, la **dirección** del remitente (tuya) y la **dirección** del destinatario (tu amigo).



Una **firma** confirma que el mensaje (documento o **bitcoin**) procede del remitente y NO ha sido modificado.

## Carteras de Bitcoin Desbloqueadas

### 6.2.2 ¿Cómo Recibo bitcoin On-Chain?

Para recibir **bitcoin**, necesitarás compartir la **dirección** de tu billetera **Bitcoin** con el remitente. Esta es una cadena única de letras y números que identifica tu billetera en la **red de Bitcoin**. Puedes encontrar la **dirección** de tu billetera iniciando sesión en ella y buscando una opción para "Recibir" o "Depositar" **bitcoin**.

Hay varias formas en que puedes compartir tu **dirección** de **Bitcoin** con el remitente:

- **Copiar y pegar la dirección:** Puedes copiar la **dirección** resaltándola y presionando "Copiar" en tu teclado. Luego, puedes pegarla en un correo electrónico o mensaje para el remitente.
- **Compartir un enlace a tu dirección de billetera Bitcoin:** Algunas billeteras de **Bitcoin** permiten generar un enlace que apunta a tu **dirección** de billetera que puedes compartir. Al hacer clic en este enlace, el remitente verá tu **dirección** de billetera y podrá utilizarla para enviar el **bitcoin**.
- **Compartir un código QR:** Si el remitente tiene un smartphone con una aplicación de billetera **Bitcoin**, puede escanear el código QR para obtener tu **dirección** de **bitcoin**.

Una vez que el remitente tiene la **dirección** de tu billetera **Bitcoin**, puede proceder a enviarte **sats** (la unidad más pequeña de **bitcoin**). Para hacerlo, el remitente introducirá tu **dirección** y la cantidad de **sats** que desea enviarte, y luego iniciará la **transacción**. Es importante recordar que, aunque verás el nuevo saldo en tu billetera una vez que la **transacción** se confirme en la **red de Bitcoin**, en realidad no "posees" los **bitcoin** en un sentido físico. En lugar de eso, tienes las llaves que te permiten mover y gastar esos **sats**. El proceso de confirmación puede durar desde unos minutos hasta varias horas, dependiendo de la tarifa de **transacción** que el remitente elija pagar y de la cantidad de tráfico en la **red de Bitcoin** en ese momento.

### 6.2.3 Ejercicio de Clase: Cómo Enviar bitcoin y Pagar Bienes y Servicios On Chain

#### Ejercicio

Para enviar **bitcoin**, necesitarás algunas cosas: una billetera de **Bitcoin**, la **dirección** de **Bitcoin** del destinatario y la cantidad de **bitcoin** que quieras enviar.

1. Abre tu billetera de **Bitcoin**. Un código SMS será enviado a tu número de teléfono, y tendrás que introducirlo en la caja de diálogo. Alternativamente, si has habilitado Google 2FA, necesitarás introducir el código de seis dígitos de la aplicación Google Authenticator.
2. Navega a la función de "Enviar" o "Retirar" y copia la **dirección** del destinatario.



3. Ingresa la **dirección** de **Bitcoin** del destinatario pegándola en el campo "A".
4. Introduce la cantidad de **bitcoin** que quieras enviar en el campo "Cantidad".
5. Revisa una vez más la **dirección** del destinatario y la cantidad a enviar.
6. Antes de hacer clic en Confirmar y Enviar, te recomendamos que verifiques los detalles de la **transacción** una vez más para asegurarte de que estás enviando la cantidad correcta de **bitcoin** a la **dirección** de billetera correcta.
7. Confirma la **transacción** y espera a que la red confirme la **transacción**.

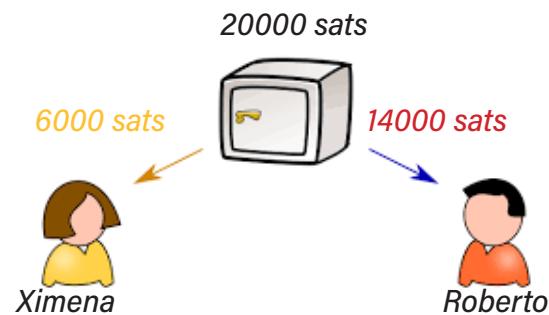
Más tarde volvemos a revisar cuantas confirmaciones tiene nuestra **transacción**.

¡Practiquemos! Vayamos a la cafetería para comprar snacks con **bitcoin**. Recuerda, es importante que sientas confianza en cada paso del proceso. ¡Diviértete aprendiendo sobre **Bitcoin** y cómo usarlo en el mundo real!

### 6.3 **Lightning Network** - Una solución para transacciones rápidas y económicas



La **Red Lightning** funciona estableciendo una cartera compartida donde ambas partes almacenan su **bitcoin** y luego tienen la flexibilidad de realizar **transacciones** ilimitadas entre ellas sin tocar la **cadena de bloques** principal. Cuando terminan, el saldo final se registra en la **cadena de bloques** principal.



La **Red Lightning** es un sistema de pagos que funciona en paralelo con la **blockchain** de **Bitcoin**. Permite a los usuarios enviar y recibir pagos de forma prácticamente instantánea utilizando **bitcoin**. Al operar fuera de la cadena principal de **Bitcoin**, la **Red Lightning** agiliza el proceso de **transacción** y reduce las tarifas asociadas.

Las **transacciones** en la **Red Lightning** se pueden realizar entre dos partes que tienen un canal de pago abierto o, incluso, pueden ser enrutadas a través de múltiples canales. Esto permite que las **transacciones** fluyan de manera ágil entre participantes que no tienen un canal directo entre ellos. En consecuencia, la **Red Lightning** ofrece una gran flexibilidad y eficiencia para realizar pagos de **bitcoin**.

# Carteras de Bitcoin Desbloqueadas

En cuanto a los participantes de la **Red Lightning**, podemos clasificarlos en tres categorías principales:

- **Usuarios:** Los usuarios son las personas o entidades que utilizan la **Red Lightning** para enviar y recibir pagos en **bitcoin**. Pueden ser usuarios regulares, comerciantes o empresas que buscan aprovechar las **transacciones** más rápidas y económicas que ofrece la **Red Lightning**. Los usuarios interactúan con la **Red Lightning** a través de billeteras o aplicaciones específicas diseñadas para esta red.
- **Clientes (Billeteras Lightning):** Estas son aplicaciones de software que facilitan la interacción del usuario con la **Red Lightning**. Los clientes gestionan la experiencia del usuario, permitiéndoles administrar sus fondos, realizar **transacciones** y observar el estado de sus pagos. Es importante señalar que los clientes no tienen una función en el enrutamiento de los pagos en la red.
- **Nodos:** Los nodos son servidores que constituyen la infraestructura de la **Red Lightning**. Tienen una doble función: mantener abiertos los canales de pago y encargarse del enrutamiento de las **transacciones** a través de la red. En otras palabras, los nodos son los que realmente procesan y dirigen las **transacciones** desde el emisor hasta el receptor.

## Las Remesas

La **Red Lightning** no solo facilita **transacciones** rápidas y económicas para el uso diario, sino que también ha ganado relevancia como una herramienta importante para las **transacciones** internacionales, como las remesas.

Figura 8 Un escenario posible del uso de costos provenientes de **Lightning** por pagos de remesas en otros países pobres y dolarizados hasta el 2030





Gracias a su capacidad para procesar pagos casi instantáneamente y con tarifas mínimas, la **Red Lightning** se ha convertido en una alternativa eficiente y económica para enviar dinero a través de las fronteras. Esto beneficia especialmente a aquellos que dependen de las remesas para sus necesidades básicas, ya que evita altas comisiones y largos tiempos de espera.

Además, la **Red Lightning** no se ve limitada por restricciones geográficas, lo que la convierte en una herramienta poderosa para realizar **transacciones** internacionales sin las barreras tradicionales de los sistemas financieros convencionales.

### 6.3.1 Monederos de la **Red Lightning**

Aunque es cada vez más común que muchos monederos ofrezcan servicios tanto en cadena (on-chain) como fuera de la cadena (**off-chain**), los monederos específicos de la **Red Lightning** y los monederos de **Bitcoin** tradicionales presentan diferencias significativas. Los monederos de la **Red Lightning** son aplicaciones que permiten a los usuarios interactuar con la **Red Lightning** para realizar **transacciones** de **bitcoin** de manera rápida y con tarifas reducidas.

Dicho esto, es importante tener en cuenta las diferencias clave entre estos dos tipos de monederos. A continuación, se presenta una comparación de algunas de estas diferencias fundamentales:

Característica	Monedero <b>Bitcoin</b> Regular	Monedero de la <b>Red Lightning</b>
Velocidad de <b>transacción</b>	Las <b>transacciones</b> pueden tardar 10 minutos o más en confirmarse	Las <b>transacciones</b> son casi instantáneas
Costo de <b>transacción</b>	Las tarifas pueden ser significativas, especialmente durante los períodos de alta demanda	Las tarifas son muy bajas, independientemente de la demanda en la red
Tamaño de <b>transacción</b>	Ideal para grandes <b>transacciones</b>	Ideal para pequeñas <b>transacciones</b> (micropagos)
Uso de recursos	No requiere recursos significativos de la red o computación	Requiere estar en línea y tener una ruta de conexión a la red para realizar <b>transacciones</b>
Privacidad	Las <b>transacciones</b> son públicas pero anónimas	Las <b>transacciones</b> son privadas y no se reflejan en la <b>blockchain</b> hasta que se cierra el canal
Seguridad	Seguridad fuerte, depende de la seguridad de la <b>clave privada</b>	Seguridad fuerte, pero depende de la vigilancia constante de la red para evitar fraudes

# Carteras de Bitcoin Desbloqueadas

## 6.3.2 Una Transacción en la Red Lightning

### Nata y Jeff: Micropagos para Acceder a Contenido de Blog a través de la Red Lightning

Nata es una lectora frecuente del blog sobre Bitcoin que Jeff administra. Jeff decide ofrecer a sus lectores una forma más rápida y cómoda de acceder a contenido premium. Cada artículo cuesta \$0.10 y Jeff también ofrece videos de tutoría por \$0.01 por minuto.

**Paso 1: Seleccionar la Billetera:** Nata elige una billetera compatible con Lightning que le resulte conveniente. Jeff también tiene una, pero no necesitan usar la misma.

**Paso 2: Financiar el Canal:** Ambos, Nata y Jeff, deciden financiar un canal de Lightning. Nata crea una transacción on-chain de \$5 para abrir el canal y Jeff decide no aportar fondos en esta instancia. La transacción se registra en la blockchain de Bitcoin.

**Paso 3: Acuerdo Colaborativo:** La apertura del canal es un proceso colaborativo. Ambos deben estar de acuerdo con los términos antes de abrirlo. La transacción inicial de \$5 de Nata se registra en el canal abierto.

**Paso 4: Realizar Micropagos:** Una vez que el canal está abierto, Nata puede realizar micropagos a Jeff para acceder a artículos y videos. Cada transacción se realiza off-chain, lo que significa que son instantáneas y no incurren en tarifas adicionales.

#### Registro de Micropagos:

Transacción	Monto	Saldo de Nata	Saldo de Jeff
Artículo 1	\$0.10	-\$0.10	+\$0.10
Minuto de video 1	\$0.01	-\$0.01	+\$0.01
...	...	...	...

**Paso 5: Cierre del Canal:** Cuando Nata decide que ya ha accedido a todo el contenido que le interesa, puede solicitar cerrar el canal. Jeff entonces firma la transacción final que actualiza la blockchain de Bitcoin con los saldos finales.

#### Registro Final:

Transacción	Monto	Saldo de Nata	Saldo de Jeff
Cierre del Canal	\$x.xx	\$5 - x.xx	+x.xx

De esta manera, Nata ha pagado a Jeff por el contenido premium en su blog y en sus videos de tutoría. Los micropagos se han realizado de forma eficiente y sin tarifas adicionales, gracias al uso del canal de Lightning.



## Capítulo #6

### Situación de Disputa

Después de unas semanas disfrutando del contenido, Nata nota que su saldo parece incorrecto. Según sus cálculos, debería tener \$2.00 restantes, pero el saldo en su billetera **Lightning** indica que sólo tiene \$1.80. Sospechando que algo ha ido mal, Nata decide cerrar el canal para resolver la disputa.

**Paso 1: Presentación de Pruebas:** Nata intenta cerrar el canal con un saldo que ella cree es correcto, enviando una **transacción** de cierre a la **blockchain** de **Bitcoin** que dice que ella tiene \$2.00 restantes. Jeff recibe una notificación sobre el intento de cierre del canal y se da cuenta de la discrepancia.

Jeff presenta su versión de las **transacciones**, que indican que Nata debería tener sólo \$1.80 restantes. Ambas partes han estado firmando cada **transacción** realizada, por lo que existe un registro de todas las **transacciones** efectuadas.

**Paso 2: Verificación de la Red Lightning:** La **Red Lightning** interviene para revisar las pruebas presentadas por ambas partes. Examina todas las **transacciones** firmadas y acordadas por Nata y Jeff para determinar cuál es el saldo correcto.

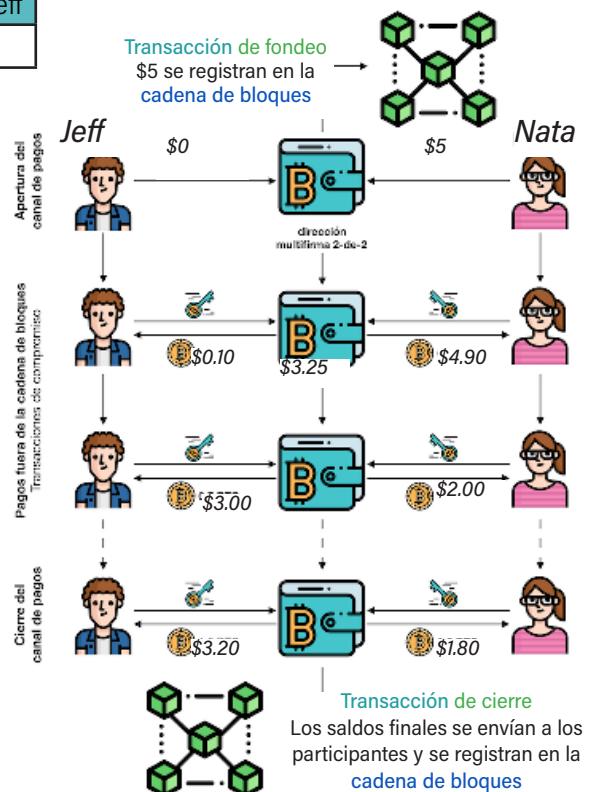
**Paso 3: Resolución de la Disputa:** Tras la revisión, la **Red Lightning** determina que el saldo correcto de Nata es de \$1.80. La **transacción** de cierre se ajusta de acuerdo a esta cantidad y se registra en la **blockchain** de **Bitcoin**.

### Registro Final Post-Disputa:

Transacción	Monto	Saldo de Nata	Saldo de Jeff
Resolución de Disputa	\$x.xx	\$1.80	\$5 - 1.80

Nata aprende una valiosa lección sobre la importancia de mantener un registro detallado de sus **transacciones**, y Jeff se siente más seguro sabiendo que la **Red Lightning** puede manejar disputas de forma justa.

De esta manera, incluso en el caso de un desacuerdo sobre los saldos, la **Red Lightning** proporciona un mecanismo para resolver disputas de manera efectiva, manteniendo la integridad del sistema.



# Carteras de Bitcoin Desbloqueadas

## 6.3.3 Actividad: Carrera de Relevos de Billeteras Lightning

1. Descarga e instala una Billetera **Lightning** en tu teléfono u ordenador. Hay varias opciones disponibles, como Breez, **Bitcoin** Beach Wallet, Phoenix y Eclair para teléfonos móviles, y **Lightning** App y Zap para ordenadores de sobremesa.
2. Sigue las instrucciones para configurar el monedero. Esto puede implicar crear un nuevo monedero o restaurar uno existente, y asegurarlo con una contraseña u otra forma de autenticación.
3. Asegúrate de que tengas forma de recibir **satoshis**, como proporcionar una **dirección** de recepción o escanear un código QR proporcionado por tu profesor o compañero de grupo.
4. Cuando tu monedero esté listo y estés preparado para recibir **satoshis**, tu profesor te dará a ti y a tu grupo una cantidad inicial de **satoshis** enviándolos directamente a tu monedero.
5. El objetivo de tu grupo es pasar los **satoshis** de un monedero a otro utilizando la red **Lightning**, hasta llegar a la última persona del grupo.
6. Para enviar **satoshis** a otra persona, abre tu monedero y sigue las instrucciones para realizar un pago. Facilita la factura **Lightning** del destinatario o escanea un código QR, e introduce la cantidad de **satoshis** que deseas enviar.
7. Si tu grupo es el primero en enviar con éxito los **satoshis** a la última persona, ¡ganas! También puedes quedarte con los **satoshis** y recibir algún caramelo como recompensa.

Comparación entre Pagos en **Red Lightning** y el Sistema Bancario Tradicional

Beneficios	<b>Lightning</b>	Sistema Bancario Tradicional
Velocidad	Rápido	Lento
Transparencia	Transparente	Opaco
Seguridad	Seguro	Vulnerable
Tarifas de Transacción	Bajas	Altas
Inclusión Financiera	Alta	Limitada

Comparación entre Pagos en **Red Lightning** y en la Cadena de Bloques (On-Chain)

Beneficios	<b>Lightning</b>	On-Chain
Escalabilidad	Alta	Baja
Privacidad	Alta	Moderada
Interoperabilidad		Baja
Cumplimiento Legal	Moderado	Alto
Costo-Efectividad	Alta	Moderada

*Visa, Inc.*



En promedio 1.700 **transacciones** por segundo.

Capacidad de 65.000 **transacciones** por segundo.



**Bitcoin On-chain**

Capacidad de 7 **transacciones** por segundo.

**Bitcoin Lightning Network**



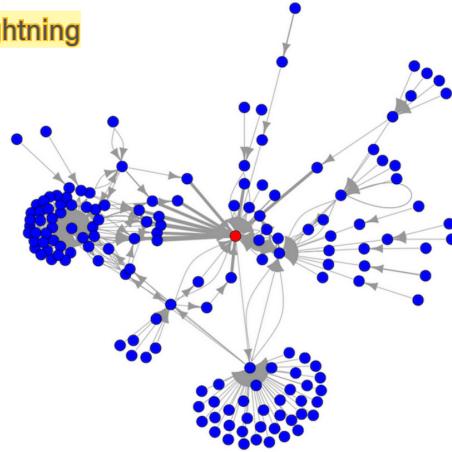
Millones de **transacciones** por segundo.



## Capítulo #6

### 6.3.4 Ejercicio de Clase: Demo Interactivo en línea de Lightning

1. Presta atención a los conceptos clave discutidos en clase, como canales de pago, rutas y tarifas.
2. Toma nota de cualquier pregunta o dificultad que encuentres al explorar el sitio web.
3. Trabaja con tu grupo para compartir tus hallazgos y discutir cualquier pregunta con la clase.
4. Prepárate para participar en discusiones en clase sobre la **Red Lightning** y su potencial como solución de escalado para **transacciones** de **bitcoin**.



**Ejercicio de Clase.** Empieza por explorar uno de los sitios web interactivos proporcionados por el profesor:

<https://lnrouter.app/graph/zero-base-fee>

<https://www.robtex.com/lnevaluator.html?conf=A5-5B,B5-5C&send=A2C>



Muchos comercios en línea están empezando a aceptar pagos con **Lightning**. Busca el logotipo de la **Lightning Network** o pregunta sobre las opciones de pago con **Lightning** al realizar compras en línea.

Algunas tiendas físicas, especialmente en ciudades con mentalidad tecnológica, también podrían aceptar pagos con **Lightning**. Mantente atento a los letreros o pregunta si aceptan **bitcoin** a través de la **Lightning Network**.

Algunos creadores de contenido, como bloggers o artistas, aceptan pagos con **Lightning** para ofrecer acceso exclusivo a su contenido o obras de arte.

Si te gustan los videojuegos, algunas plataformas y servicios de juegos están comenzando a ofrecer opciones de pago con **Lightning** para compras dentro del juego o suscripciones.

Algunas organizaciones benéficas aceptan donaciones con **Lightning**, lo que te permite apoyar causas importantes utilizando la **Lightning Network** de **Bitcoin**.



# Capítulo #7

## Descubriendo la Seguridad de Bitcoin: Las Matemáticas, el Mempool y los UTXO

7.0 El Problema del Doble Gasto y la Solución de  
Bitcoin

7.1 La Importancia de las Funciones: Las Recetas  
Transformadoras de Bitcoin

7.2 Mempool: El Guardián contra el Doble Gasto

7.3 El Papel Crucial de la Criptografía en Bitcoin

7.4 Descifrando la Criptografía de Hash

    7.4.1 Uso de Hashes y Criptografía

    7.4.2 Ejercicio de Criptografía

7.5 Rastreando la Trayectoria de tu Moneda

    7.5.1 Ejercicio. Explorando Transacciones  
        No Confirmadas

# Descubriendo los Secretos del Funcionamiento Interno

## 7.0 El Problema del Doble Gasto y la Solución de Bitcoin

11001000 11110011 01001111 11111010 00001110 11111111 01011010 00010110 00011001 00001010 01010110 01000100 00011011 1100100011111000  
10100001 01110101 10110000 00101010 10010100 01100101 11011011 00011001 01101001 00101101 10001001 11111111 10001110 00101111 10100000

¿Ves esa larga cadena de unos y ceros arriba? Se llama número aleatorio, y si lo convertimos a nuestro sistema decimal habitual, se convierte en un número con más de 256 dígitos, ¡lo cual es incluso más átomos de los que hay en nuestro universo! Sin embargo, podemos utilizar un sistema diferente para representar este número de una manera más corta, lo que llamamos **clave privada**.

Lo fascinante de esta **clave privada** es su unicidad. Nunca ha sido usada antes y jamás se repetirá después de que dejes esta página o generes una nueva. Es tan improbable como lanzar 256 monedas al aire y obtener la misma secuencia de caras y sellos dos veces, ¡Prácticamente imposible!

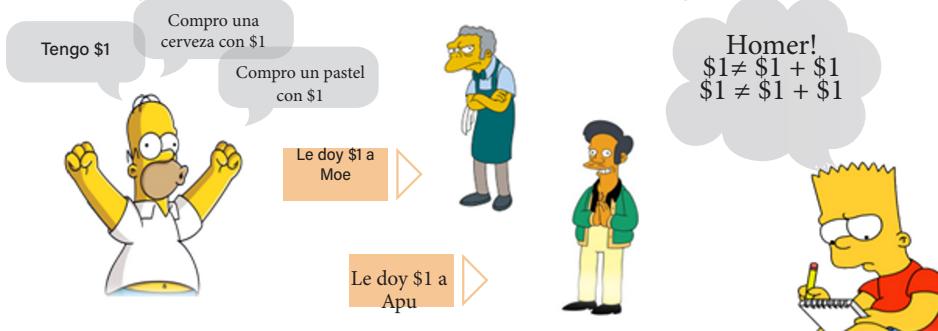
La seguridad de **Bitcoin** se asienta en la privacidad y complejidad de esta clave. Si alguien más la obtiene o si la pierdes, tu dinero será irrecuperable. ¡Así que cuídala!

¿Pero cómo protege **Bitcoin** tu **clave privada** y cómo se usa para procesar **transacciones**? Exploraremos estas cuestiones en las siguientes secciones, donde nos sumergiremos en las funciones unidireccionales, la criptografía de **clave pública** y cómo **Bitcoin** ha resuelto con maestría y de manera descentralizada el problema del doble gasto.

La realidad es que, cuando envías **bitcoins** a otra persona, debes aprobar la **transacción** con tu **clave privada**. Luego, la red verifica la autenticidad de tu **firma** para asegurarse de que todo es legítimo antes de transferir los **bitcoins**.

**Bitcoin** ha representado una solución ingeniosa a uno de los problemas más importantes de la economía digital: el **doble gasto**. Este problema, inherente al mundo digital donde la información puede duplicarse fácilmente, implica el riesgo de gastar la misma cantidad de dinero digital dos veces. Para apreciar la importancia de esta cuestión, necesitamos comprender cómo funcionan los sistemas de dinero tradicionales y por qué las soluciones a este problema en esos sistemas no son aplicables al mundo digital.

En el mundo físico, el problema del doble gasto se soluciona con la tangibilidad del dinero. Si entregas un billete de diez dólares a un camarero para pagar tu café, ese billete ya no está en tu posesión para gastarlo de nuevo. Es sencillo. Pero en el mundo digital, las cosas funcionan de manera diferente y aquí es donde **Bitcoin** brilla.



Sin embargo, en el mundo digital, la situación es drásticamente diferente. Supón que tienes un archivo que representa un **bitcoin** y decides enviárselo a una amiga como regalo de cumpleaños. Este archivo se copia a su computador, pero sigue existiendo en el tuyo. Luego, te das cuenta de que también le debes dinero a tu exnovio y decides enviarle el mismo archivo. Ahora ambos, tu amiga y tu exnovio, tienen una copia del mismo **bitcoin**. Aquí surge el dilema: ¿cómo puede un sistema de dinero digital descentralizado determinar cuál de estas **transacciones** ocurrió primero, o si es legítimo que ambas **transacciones** ocurran?

Los sistemas de dinero digital centralizados, como los bancos, resuelven este problema a través del control centralizado. Cada **transacción** pasa por el banco, que actúa como un intermediario de confianza, asegurándose de que cada cantidad de dinero se gaste solo una vez. Sin embargo, en un sistema descentralizado como **Bitcoin**, no hay una entidad central que pueda mantener un registro de todas las **transacciones** y evitar el doble gasto.

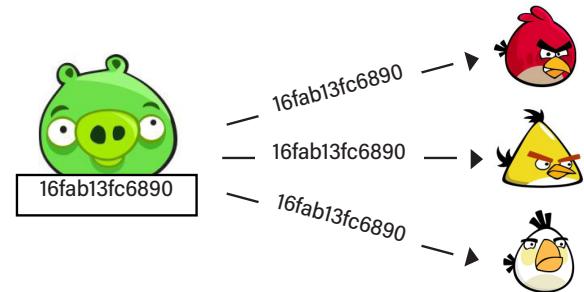
#### ¿Cómo evita la red las **transacciones conflictivas**?

Los nodos de la red identifican y sólo aprueban una de estas **transacciones** basándose en las "reglas de consenso". Si, por ejemplo, intentas gastar el mismo **bitcoin** dos veces, la **transacción** más tardía probablemente será rechazada. La elección de qué **transacción** se aprueba primero depende en gran medida de cuál recoge un minero antes. Las reglas de consenso por lo tanto son:

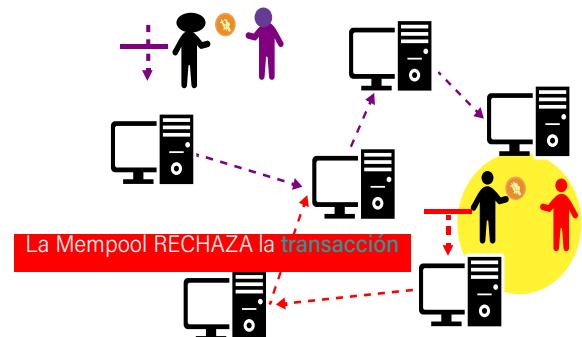
- **Prueba de Trabajo:** Los mineros deben resolver un **rompecabezas matemático** para agregar nuevas **transacciones** a la cadena. Es un trabajo duro que desalienta el juego sucio.
- **La regla de la cadena más larga:** Si hay dos cadenas de bloques en conflicto, la red elige la más larga. Ayuda a prevenir el doble gasto y mantiene las **transacciones** seguras.
- **Ajuste de dificultad:** El rompecabezas matemático cambia su dificultad cada dos semanas para mantener un ritmo de un bloque cada 10 minutos. Si se generan bloques muy rápido, el rompecabezas se hace más difícil.
- **Recompensas y tarifas por transacción:** Los mineros obtienen **bitcoins** y tarifas de **transacción** por el trabajo que hacen.
- **Limitación del tamaño de los bloques:** Los bloques en **Bitcoin** tienen un límite de tamaño, lo que limita cuántas **transacciones** se pueden agregar a cada bloque.

En resumen, **Bitcoin** evita el doble gasto usando reglas, energía, criptografía y cooperación en la red. Usa un sistema llamado UTXO para rastrear todos los fondos y prevenir el doble gasto. Todo esto asegura que **Bitcoin** funcione sin una autoridad central. Ahora, vamos a explorar más sobre cómo **Bitcoin** logra esto en la próxima sección.

#### *El Problema del Doble Gasto*



*¡Los bits son más fáciles de copiar que el papel!*



# Descubriendo los Secretos del Funcionamiento Interno

## 7.1 La Importancia de las Funciones: Las Recetas Transformadoras de Bitcoin

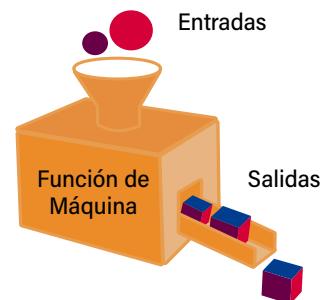
Nuestra expedición en el universo **Bitcoin** nos lleva ahora a explorar las **funciones**, elementos críticos que garantizan la correcta ejecución de las **transacciones**. Estas 'reglas y procesos' previenen el doble gasto, asegurándose de que los **bitcoins** gastados pertenezcan legítimamente al remitente y no se hayan utilizado previamente. Para lograr esto, utilizan el registro completo de todas las **transacciones** anteriores, que se guarda en ese libro contable compartido que hemos mencionado varias veces: la **blockchain** de Bitcoin.



En términos simples, una **función** es como una máquina o una caja negra que convierte cierta información en algo nuevo. La información que se le proporciona a la función se llama **entrada**, y la nueva información que la función produce es la **salida**.

Aunque pueda parecer un tema técnico, las funciones son indispensables, sosteniendo la seguridad y confiabilidad del sistema **Bitcoin** a través de:

- **Validación:** Aseguran que solo el dueño del **bitcoin** pueda gastarlo.
- **Integridad:** Utilizan códigos únicos para vincular cada bloque con su predecesor, salvaguardando la información.
- **Doble gasto:** Detectan intentos de gastar dos veces la misma moneda gracias a estos códigos únicos.
- **Direcciones de Bitcoin:** Generan **direcciones** de **Bitcoin** para proporcionar mayor seguridad.



Además, en **Bitcoin**, las funciones actúan como chefs en una cocina digital, combinando diversos ingredientes para crear algo totalmente nuevo. Cada **transacción** en **Bitcoin** se asemeja a una receta de cocina, teniendo entradas (UTXOs) y generando salidas. Cada UTXO, o ingrediente, tiene un valor en **Bitcoin** y debe ser 'consumido' para ser usado en una **transacción**. Al igual que un chef crea un plato completamente nuevo a partir de los ingredientes proporcionados, las funciones en **Bitcoin** toman estos UTXOs, los 'consumen' y, en el proceso, producen nuevos UTXOs.



## 7.2 Mempool: El Guardián contra el Doble Gasto

Cada **transacción** de **Bitcoin** pasa por un proceso de verificación antes de integrarse en la **cadena de bloques**. La mempool, o grupo de memoria, es una parte integral de este proceso.

Cuando se realiza una **transacción**, no se incorpora inmediatamente a la **blockchain** permanente. Primero, se almacena temporalmente en la mempool de los nodos de la red, una especie de sala de espera donde se verifica cada **transacción**.

En esta sala de espera, la mempool actúa como un guardián, protegiendo la red contra el doble gasto. Sin este sistema de comprobación, un **bitcoin** podría usarse en varias **transacciones**, amenazando la integridad del sistema. Por tanto, la mempool garantiza que cada **bitcoin** se gaste una sola vez.

Cuando un nodo recibe por primera vez una **transacción** de un par, debe verificar que la **transacción** sea legítima. Nadie quiere **transacciones** defectuosas o engañosas.



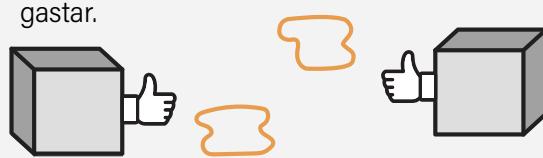
Un *mempool* es donde las **transacciones** esperan ser confirmadas en un bloque.

En la mempool, las **transacciones** son validadas mediante un proceso denominado "Accept To Memory Pool" (ATMP), que significa "aceptar en el grupo de memoria". Durante el proceso ATMP, los nodos revisan varios aspectos, como:

- ¿Ya se ha recibido esta **transacción**?
- ¿Existe algún conflicto con una **transacción** diferente en la mempool?
- ¿El **bitcoin entrante** cubre el **bitcoin saliente**?
- ¿Las firmas prueban que se pueden gastar las salidas anteriores?
- ¿Son suficientes las tarifas?

1

Retransmitir **transacciones** **no** confirmadas. Es decir, **transacciones** de dinero que se pueda gastar.



2

Proporcionar **transacciones** a los mineros.

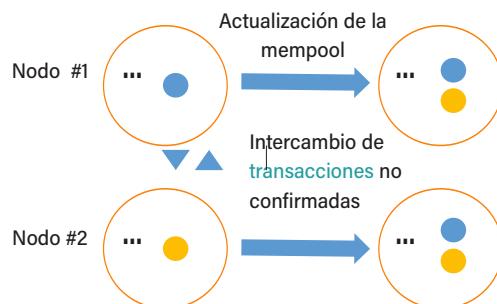


# Descubriendo los Secretos del Funcionamiento Interno



La sincronización de Mempool es un proceso mediante el cual los nodos en la red intercambian información sobre las **transacciones** que cada uno ha verificado pero que aún no se han añadido a la **cadena de bloques**.

Una vez validada, la **transacción** espera en la mempool a ser seleccionada por un minero para su inclusión en el próximo bloque y su registro definitivo en la **blockchain**. No obstante, una **transacción** puede ser rechazada por diversas razones, como tarifas insuficientes, congestión de la red o errores en los datos de la **transacción**. En tales casos, los **bitcoins** no se pierden y finalmente se devuelven al monedero del remitente.



## 7.3 El Papel Crucial de la Criptografía de Claves públicas

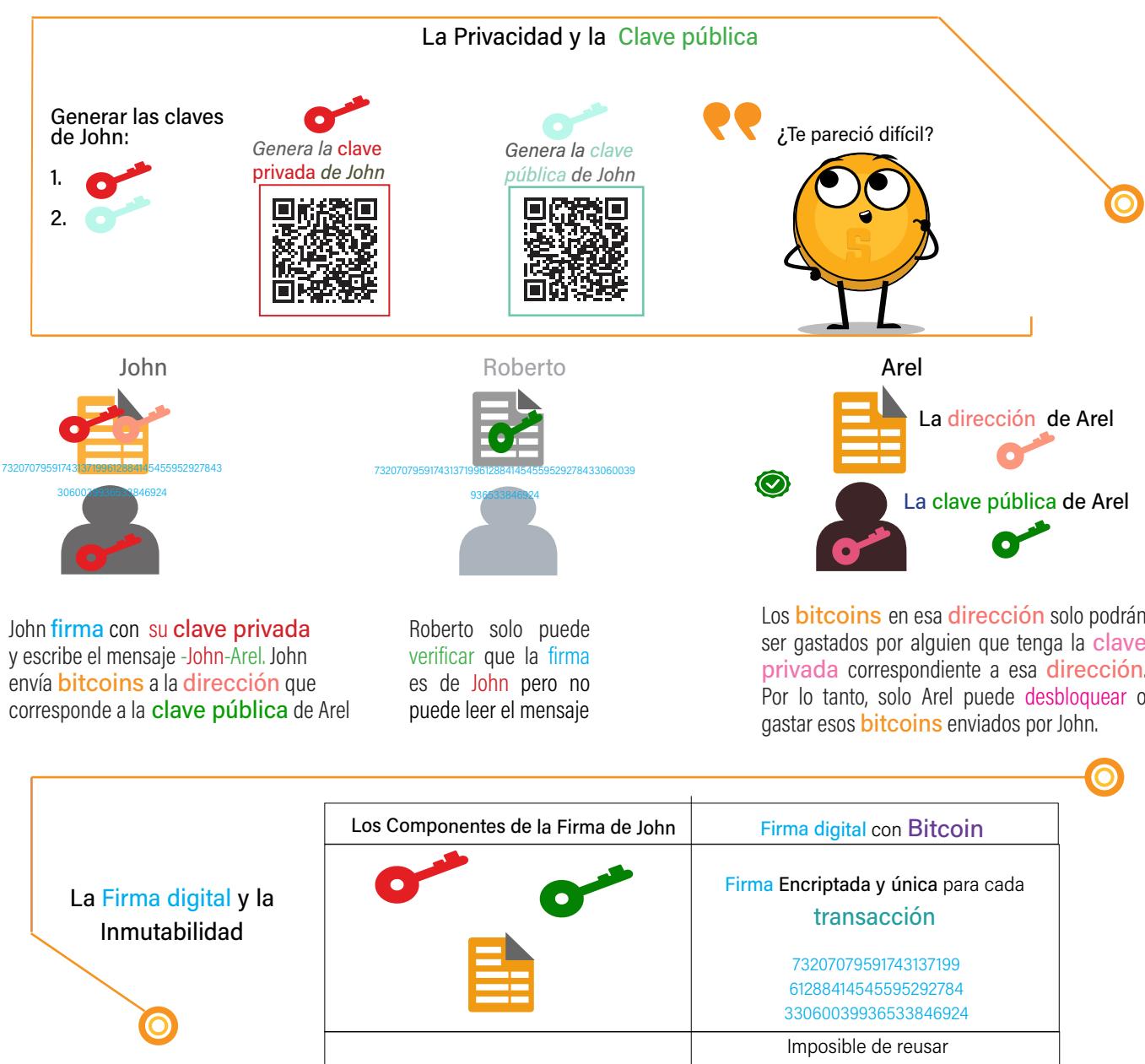
Una vez familiarizados con el problema del doble gasto y la mempool, así como su interrelación, estamos listos para profundizar en un tema fundamental: la criptografía. Este elemento es clave en el esquema de **Bitcoin**, garantizando que las **transacciones** sean seguras, genuinas y a prueba de manipulaciones. En **Bitcoin** se utilizan principalmente dos tipos de criptografía: la de **claves públicas** y la criptografía hash.

En **Bitcoin**, se utiliza un sistema de criptografía de **claves públicas**. Imaginemos a John y Arel, que necesitan compartir un PIN de seguridad sin que Roberto se entere. Deciden cifrar su comunicación utilizando una clave secreta, como desplazar cada letra del mensaje un espacio en el alfabeto. Solo aquellos con la clave pueden descifrar el mensaje, manteniéndolo incomprendible para Roberto.

En el contexto de **Bitcoin**, John y Arel tienen cada uno un par de claves: una **clave privada** y una **clave pública**. La **clave privada** se mantiene en secreto, mientras que la **clave pública** es conocida por todos. Cuando John quiere enviar un mensaje a Arel, lo encripta con la **clave pública** de Arel. Solo la **clave privada** de Arel puede descifrar el mensaje. Esto asegura que solo el dueño legítimo de la **clave privada** pueda autorizar la disposición de sus **bitcoins**.

La criptografía de **Bitcoin** garantiza que solo los propietarios legítimos puedan autorizar **transacciones**, protegiendo contra el fraude y la manipulación. Las **claves privadas** y públicas, las **direcciones de Bitcoin** y las **firmas digitales** son los elementos fundamentales que salvaguardan las **transacciones** y permiten el funcionamiento seguro del ecosistema.

Por ejemplo, supongamos que John tiene 5 **bitcoins** y decide enviar 2 de ellos a su amigo Arel. En un sistema seguro, John firmará digitalmente la **transacción** con su **clave privada**, asegurando que solo él, como propietario legítimo de los **bitcoins**, pueda autorizar la **transacción**.



# Descubriendo los Secretos del Funcionamiento Interno

Ahora, existe un riesgo: si un hacker, como Roberto, logra comprometer el sistema de criptografía y falsifica la **firma digital** de John, podría cambiar la **dirección** de destino y recibir los 2 **bitcoins** destinados a Arel. Incluso podría alterar la **transacción** original y enviar 5 **bitcoins** a su propia **dirección**. Esto destacaría la importancia de un sistema de claves robusto en la criptografía.

## Analogía de la Máquina Expendedora

Imagina que **Bitcoin** es como una máquina expendedora muy confiable. Si insertas el dinero y eliges el mismo refresco, siempre obtendrás el mismo resultado: tu refresco favorito. No hay sorpresas. En el mismo sentido, cuando realizas una **transacción** en **Bitcoin** con las mismas instrucciones de entrada, siempre obtendrás el mismo resultado: una **transacción** segura y verificada. Este nivel de confiabilidad se debe a la criptografía que protege el sistema. Y aunque hay desafíos en el camino, la comunidad de **Bitcoin** sigue trabajando para fortalecer aún más la red.

¿Qué tal si intentamos nosotros mismos?



## 7.4 Descifrando la Criptografía de Hash

Además de la criptografía de **claves públicas**, **Bitcoin** también utiliza la criptografía hash para mantener la integridad y secuencia de la **cadena de bloques**. La criptografía hash genera una estructura resistente a alteraciones, lo que garantiza la fiabilidad de la **cadena de bloques**.

No hay necesidad de intimidarse con la terminología técnica y los conceptos matemáticos que vamos a desglosar a continuación. Incluso las ideas más complejas pueden ser digeridas con paciencia y dedicación.

Los sistemas binarios y hexadecimales son dos formas de representar datos numéricos. El binario sólo utiliza dos dígitos: 0 y 1, conocidos como bits, y un conjunto de 8 bits se denomina byte. El hexadecimal utiliza 16 dígitos: del 0 al 9 y las letras de la A a la F para representar los números del 10 al 15. Cada dígito hexadecimal representa 4 bits, por lo que dos dígitos hexadecimales representan un byte.

Estos sistemas son ampliamente utilizados en informática y criptografía, ya que pueden representar cualquier tipo de información, desde letras hasta frases completas, en formatos numéricos que son compatibles con los sistemas digitales.

Inténtalo tu:



Para convertir de binario a hexadecimal, se agrupan los bits de 4 en 4 desde el extremo derecho y se transforman a su correspondiente valor hexadecimal. Aquí tienes un ejemplo:



Número binario: 1010 1100 0110 0001

Agrupamos los bits de 4 en 4:

1010 (A en hexadecimal) 1100 (C en hexadecimal)  
0110 (6 en hexadecimal) 0001 (1 en hexadecimal)

Entonces el número binario 1010110001100001 se convierte en el número hexadecimal AC61.

### ¿Qué son las funciones unidireccionales?

Piensa en una función unidireccional como una receta de batido: una vez que has mezclado tus ingredientes y obtenido tu batido, no puedes revertir el proceso para recuperar los ingredientes originales. Del mismo modo, las funciones unidireccionales procesan información y la convierten en algo nuevo, pero no puedes revertir este proceso para obtener la información original.

En el caso de **Bitcoin**, estas funciones son esenciales para la criptografía de **clave pública**. Por ejemplo, las **claves públicas** se generan a partir de **claves privadas** de una manera que no puede ser revertida. Esto significa que, aunque alguien obtenga tu **clave pública**, no podrán obtener tu **clave privada**.

¿Suenas confuso?

# Descubriendo los Secretos del Funcionamiento Interno

Una función unidireccional utiliza un conjunto de instrucciones para procesar la información y convertirla en algo nuevo, al igual que una receta de batido transforma los ingredientes en una nueva bebida. Sin embargo, al igual que no puedes deshacer un batido para obtener los ingredientes originales, no puedes revertir la función unidireccional para obtener la información original.

La criptografía de **clave pública**, que incluye la **clave pública**, se basa en el uso de funciones unidireccionales, las cuales dificultan la obtención de la **clave privada** a partir de la **clave pública**. No es exactamente "imposible" encontrar la **clave privada** a partir de la **clave pública**, pero sí es extremadamente difícil y requeriría una cantidad ingente de tiempo y poder computacional para lograrlo.

Encontrar una **clave privada** a partir de una **clave pública** en **Bitcoin** es como buscar una aguja en un pajar tan grande como un campo de fútbol. La aguja representa la **clave privada** y el pajar representa todas las posibles **claves privadas**.

De la misma manera, las funciones unidireccionales están diseñadas para ser irreversibles y no pueden ser descifradas.



El hash es como una huella digital para los datos digitales. Es un proceso que toma un mensaje digital y lo transforma en un código de longitud fija, que sirve como identificador único.

## ¿Qué es un hash?

Al igual que una huella dactilar puede identificar a una persona, un hash puede identificar un mensaje digital. Los hashes son funciones unidireccionales. Esto significa que los datos que se ingresan en la función se procesan para generar un resultado único (el hash), pero este proceso no se puede revertir. En otras palabras, no puedes tomar un hash y "deshacer" la función para obtener los datos originales. Los hashes se utilizan en muchas aplicaciones, incluyendo las **transacciones** de **Bitcoin**.



Una función hash es como una máquina de códigos secretos. Toma un mensaje y lo convierte en un código.



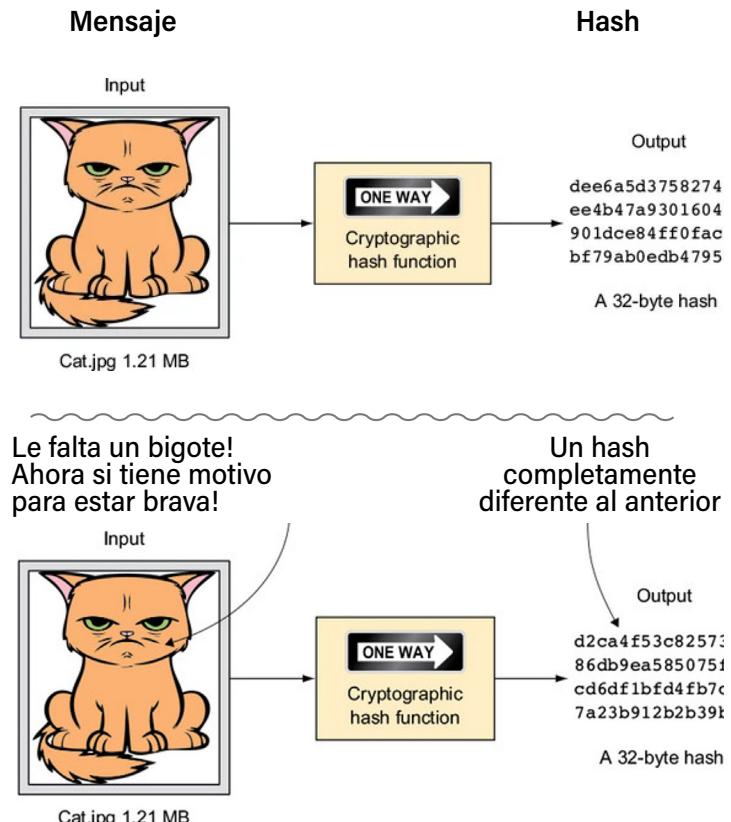
”

En este enlace encontrarás otro generador de hash donde puedes probarlo por ti mismo.

En el contexto de **Bitcoin**, los hashes son esenciales para una variedad de funciones clave, desde la prevención de fraudes hasta la verificación de **transacciones** y la vinculación de bloques en la **blockchain**. Los hashes son parte integral de la estructura y la seguridad de **Bitcoin**, y aquí se explican algunas de sus aplicaciones más importantes:

#### Identificación de **transacciones** y **bloques**:

Cada **transacción** en la **red de Bitcoin** se somete a un proceso de hashing, y el hash resultante actúa como una "**firma digital**" única para esa **transacción**. De manera similar, cada bloque en la **blockchain** también tiene un hash único que lo identifica. Este hash es calculado a partir de la información contenida en el bloque, lo que incluye las **transacciones** y el hash del bloque anterior en la cadena. Este proceso de "encadenamiento" ayuda a asegurar la integridad de la **blockchain**.



**Prevención de fraudes:** Los hashes también juegan un papel crucial en la prevención de fraudes en la **red de Bitcoin**. Si alguien intenta alterar una **transacción**, incluso en un solo detalle, el hash de la **transacción** cambiará completamente. Esto se debe a la naturaleza de las funciones de hash, que producen una salida completamente diferente incluso ante el menor cambio en la entrada. Esto hace que sea extremadamente difícil para un atacante manipular una **transacción** o un bloque sin ser detectado.

**Verificación de transacciones:** Cuando se realiza una **transacción**, se crea un hash de la **transacción** que se puede utilizar para verificar la **transacción**. Si un usuario quiere comprobar que una **transacción** ha ocurrido, puede comparar el hash de la **transacción** proporcionada con el hash en la **blockchain**. Si coinciden, entonces la **transacción** es válida y ha sido incluida en la **blockchain**.

**Prueba de trabajo:** Los hashes también son fundamentales para el proceso de "prueba de trabajo" que se utiliza en **Bitcoin**. En este proceso, los mineros compiten para resolver un problema matemático basado en una función de hash. El primer minero que resuelve el problema gana el derecho a agregar un nuevo bloque a la **blockchain** y recibe una recompensa en **bitcoins**. Esto proporciona un incentivo para que los mineros mantengan la **red de Bitcoin** segura y operativa.

En resumen, los hashes son esenciales para el funcionamiento y la seguridad de **Bitcoin**.

# Descubriendo los Secretos del Funcionamiento Interno

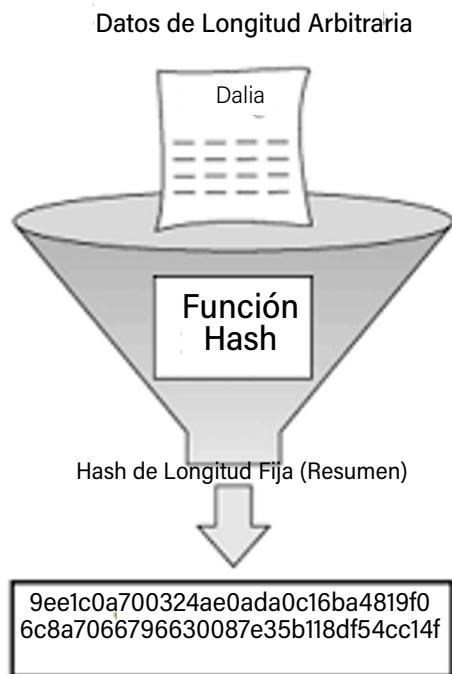
## El papel del Hashing en la Provisión de Seguridad

El hashing es fundamental para la seguridad de la **red de Bitcoin**. Los hashes identifican y validan las **transacciones**, permitiendo a la red detectar y prevenir el fraude. Este proceso asegura que todas las **transacciones** se registren de manera precisa en la **cadena de bloques**.

En **Bitcoin**, se utilizan funciones hash específicas llamadas SHA-256 y RIPEMD160. Estos algoritmos producen hashes que son únicos para cada conjunto de datos de entrada, y cualquier cambio, incluso minúsculo, en los datos de entrada resultará en un hash completamente diferente.



Genera instantáneamente un hash SHA256 de cualquier cadena o valor de entrada. Las funciones hash se utilizan como métodos unidireccionales.



Esta es mi huella DIGITAL en el mundo moderno!

## Uso de Hashes y Criptografía en la Generación de Semillas, Claves y Direcciones de BTC

Las tecnologías esenciales en **Bitcoin** incluyen las funciones de hash y la criptografía de **clave pública**. Estos son componentes críticos para la seguridad y la funcionalidad de **Bitcoin**. Veamos cómo se utilizan juntas:

**Generación de la semilla:** Todo comienza con la generación de una semilla, que es esencialmente una frase aleatoria de palabras. Esta semilla se genera utilizando un algoritmo de generación de números aleatorios.

**Creación de la clave privada:** La semilla se pasa a través de una función de hash para crear una **clave privada**. Esta **clave privada** es un número aleatorio único.

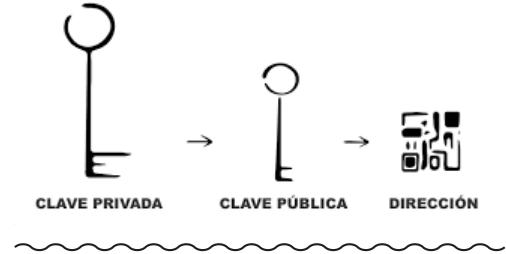
**Creación de la clave pública:** Creación de la **Clave pública:** La **clave privada** se pasa por una función matemática especial para generar una **clave pública**. A pesar de que la **clave pública** se deriva de la **clave privada**, no es posible recuperar la **clave privada** a partir de la **clave pública**, lo que proporciona un nivel de seguridad adicional.

**Creación de la dirección de Bitcoin:** La **clave pública** se pasa a través de una serie de funciones de hash para crear una **dirección** de Bitcoin. Esta **dirección** es la que se comparte y se utiliza para recibir fondos.

**Verificación de transacciones:** Al enviar una **transacción**, se utiliza la **clave privada** para crear una **firma digital**. Cualquier persona puede usar la **clave pública** para verificar esta firma y confirmar que el propietario de la **clave privada** ha autorizado la **transacción**, sin revelar la **clave privada** en sí misma.



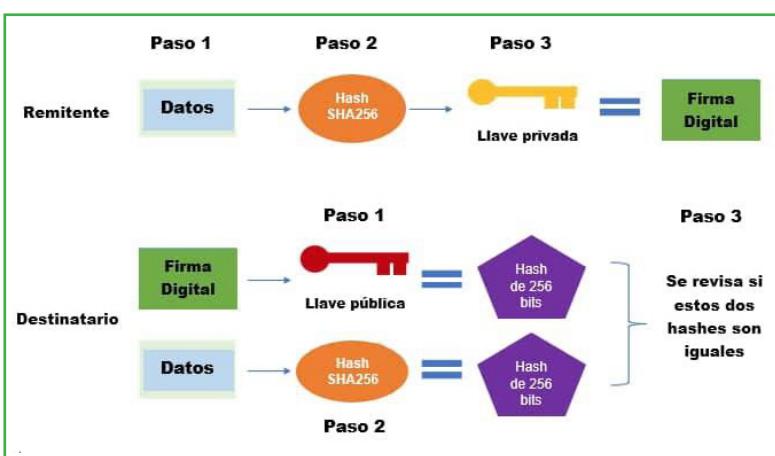
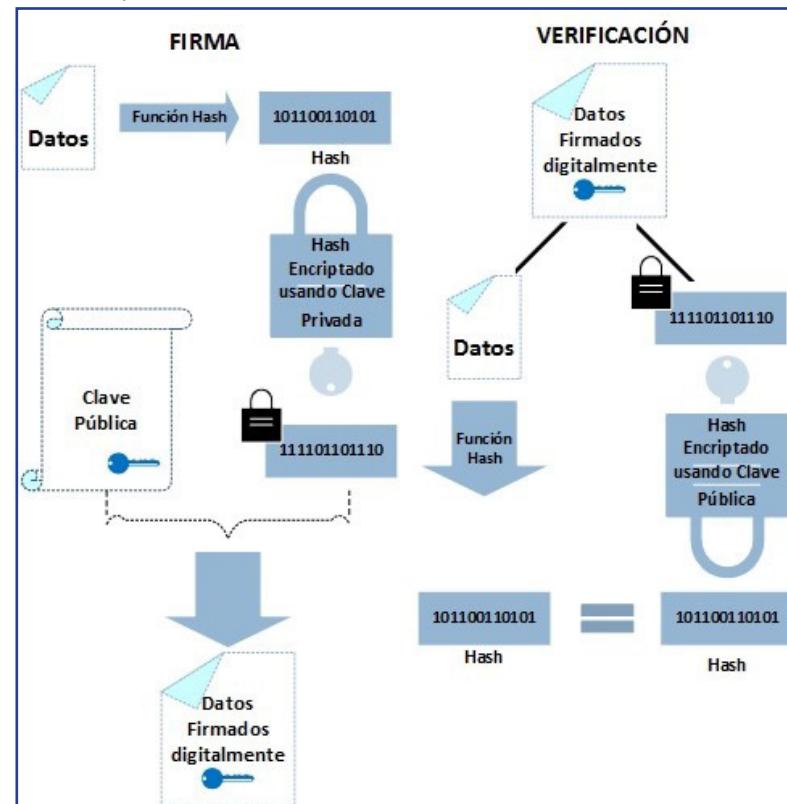
Inténtalo con  
tus compañeros.  
Encripta y de-  
cripta mensajes  
secretos.



#### 7.4.1 Ejercicio de Criptografía

Forma parejas en la clase. Cada pareja debe:

1. Generar un mensaje secreto.
2. Generar un par de claves (pública y privada).
3. Firmar el mensaje con la **clave privada**.
4. Compartir el mensaje firmado y la **clave pública** con la otra pareja.
5. La otra pareja utiliza la **clave pública** para verificar la **firma** y asegurarse de que el mensaje proviene de la pareja correcta y no ha sido alterado.
6. Las parejas pueden intercambiar mensajes firmados y verificados utilizando este esquema.



# Descubriendo los Secretos del Funcionamiento Interno

## 7.5 Rastreando la Trayectoria de tu Moneda

Después de explorar importancia de la mempool y la criptografía de **claves públicas**, vamos a abordar de nuevo el concepto del modelo de **transacciones UTXO** de **Bitcoin**. Para entender cómo funciona, piensa en **Bitcoin** como un sistema de pagos en efectivo, donde cada "moneda" o "billete" se representa como un UTXO.



¿Qué es un **UTXO**? UTXO es una sigla que significa "**Unspent Transaction Output**", que en español significa "Salida de **Transacción** No Gastada". Pero no pierdes todo tu dinero, porque cualquier cambio se convierte en un nuevo UTXO.

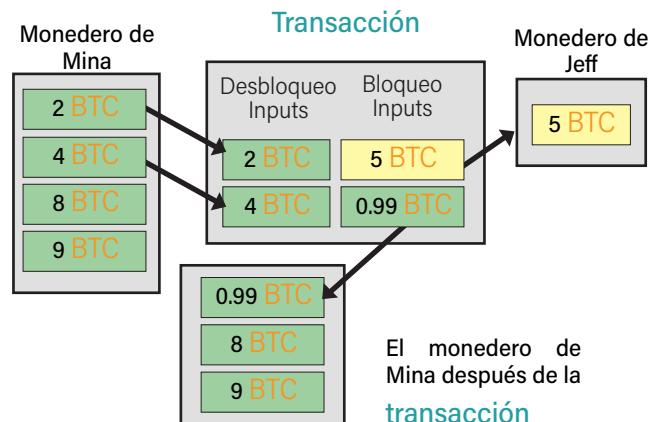
Imagina que quieres comprar un helado que cuesta \$2,000 pesos y pagas con un billete de \$5,000. No puedes cortar el billete, por lo que pagas todo y el billete de \$5000 se considera gastado. Luego, el vendedor te da \$3000 pesos de cambio, que representan tu nuevo UTXO, un nuevo "billete" que puedes usar para futuras **transacciones**.

El modelo UTXO aporta transparencia y trazabilidad a las **transacciones**, permitiendo a cualquier observador verificar la validez de una **transacción** simplemente examinando el **blockchain**. Además, garantiza la prevención del doble gasto, ya que cada UTXO solo puede ser gastado una vez.

Veamos varios ejemplos con **Bitcoin**:

1. Digamos que Mina desea enviar 5 **BTC** a Jeff. Mina tiene 4 UTXOs, que suman un total de 23 **bitcoins**. Para realizar la **transacción**, Mina "gasta" 6 de sus **bitcoins** (como si entregara un billete de 6 **bitcoins**), envía 5 a Jeff y 0.99 de vuelta a ella misma, con una tarifa de procesamiento de 0.01. Este cambio de 0.99 **bitcoins** se convierte en un nuevo UTXO que Mina puede gastar en el futuro.

Si Mina intenta luego enviar 19 **BTC** a Ximena, la **red de Bitcoin** rechazaría la **transacción**. Esto se debe a que algunos de los UTXOs que Mina utilizó para pagar a Jeff ya se han "gastado", y no pueden volver a gastarse.

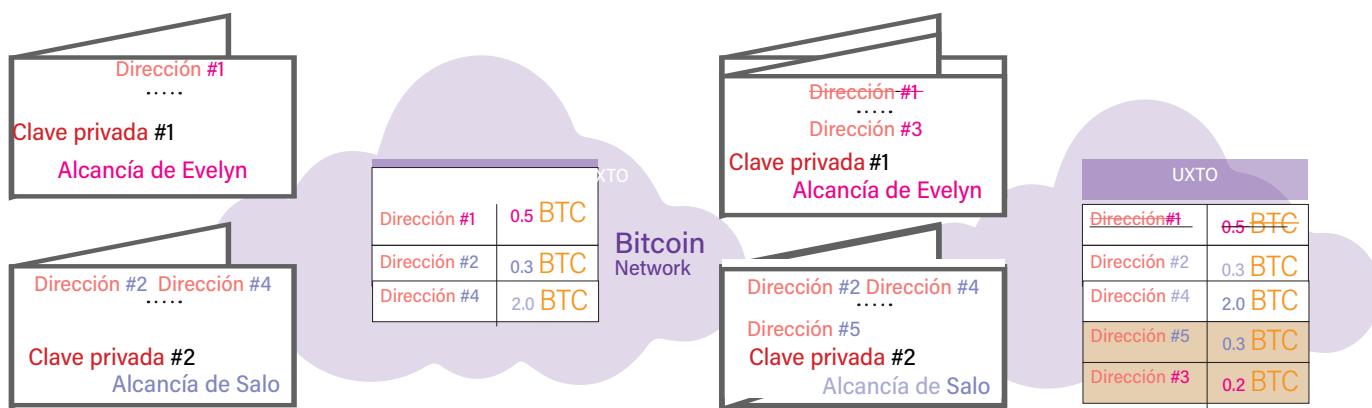


\*Una nueva UTXO de 0.01 se ha mandado a un minero.

2. Para entender mejor la relación entre los UTXOs y la criptografía de **clave pública** en **Bitcoin**, podemos pensar en una analogía de un candado y una llave.

Imaginemos que Evelyn tiene una **alcancía** virtual (un UTXO) con 0.5 **BTC**. Decide enviar 0.3 **BTC** a Salo. Aquí es donde las cosas se vuelven interesantes en el mundo **Bitcoin**:

1. Evelyn no puede simplemente sacar 0.3 **BTC** de su **alcancía** de 0.5 **BTC**. En vez de eso, debe "romper" toda la **alcancía** y decidir cómo se redistribuirá.
2. Así que, de esos 0.5 **BTC**, 0.3 **BTC** van a una nueva **alcancía** que Salo acaba de crear para recibirlas (llamémosla **alcancía #5**).
3. Pero Evelyn no quiere perder su cambio, por lo que crea una nueva **alcancía** para sí misma, y en ella pone los 0.2 **BTC** restantes.



4. Ahora, para asegurarse de que solo Salo pueda usar esos 0.3 **BTC**, se coloca un "candado especial" en la "**alcancía**" #5, que solo Salo puede abrir con su llave especial (**llave privada**).
5. Lo mismo ocurre con la **dirección** de cambio de Evelyn: se pone un candado que solo ella puede abrir.

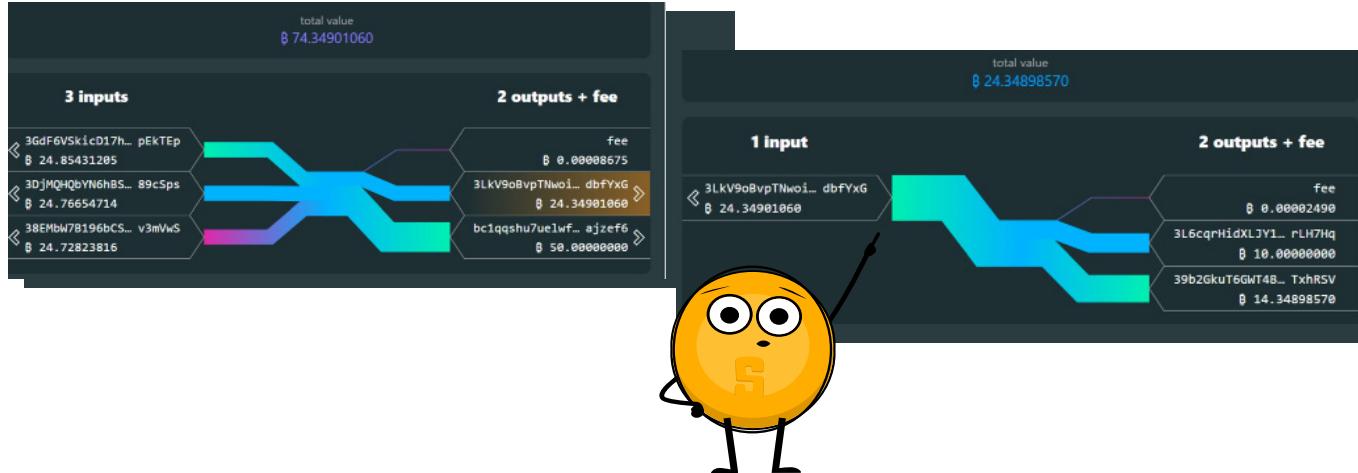
Una vez que la **transacción** se registra en la **cadena de bloques**, que funciona como un libro de contabilidad descentralizado, el monedero de Salo muestra un total de 2.6 **bitcoins**, mientras que el monedero de Evelyn muestra 0.2 **bitcoins**, ahora asociados a su nueva **dirección** (#3).

Y un pequeño detalle que dejamos de lado: al realizar esta operación, Evelyn paga una pequeña tarifa a un "guardián" (minero) para que registre esta **transacción** en el gran libro contable del **Bitcoin**, la **cadena de bloques**. Pero entraremos en detalles sobre esto más adelante.

Por lo tanto, gracias a las **claves privadas** y a la generación de nuevos UTXOs, **Bitcoin** garantiza la seguridad y la propiedad exclusiva de las **transacciones** y los saldos. Sin embargo, es esencial que Evelyn mantenga sus **claves privadas** en secreto. Si estas claves caen en las manos equivocadas, sus candados podrían ser abiertos y sus **bitcoins** gastados sin su consentimiento.

# Descubriendo los Secretos del Funcionamiento Interno

3. A continuación, encontrarás una captura de pantalla de una **transacción** de Bitcoin real. Esta **transacción**, en particular, sólo tiene un input. No obstante, en muchas **transacciones**, el balance inicial podría provenir de múltiples UTXOs acumulados en **transacciones** anteriores.



Fíjate bien en los detalles de la **transacción**. ¿Coinciden los inputs con los outputs? ¿Puedes identificar los detalles específicos de la **transacción**, como las **direcciones** involucradas y las cantidades transferidas? ¿Existe alguna conexión o patrón que puedas identificar entre los inputs y outputs?

Además, podrás observar dos capturas de pantalla, cada una representando una **transacción** diferente. ¿Puedes identificar cuál de estas **transacciones** ocurrió primero? Recuerda, cada **transacción** en la **cadena de bloques** lleva un sello de tiempo, que puede ser útil para determinar la secuencia de las **transacciones**.

Asegúrate de entender cómo funciona el sistema UTXO y cómo se refleja en estas **transacciones**. Este conocimiento será fundamental para entender cómo se rastrean los **bitcoins**.

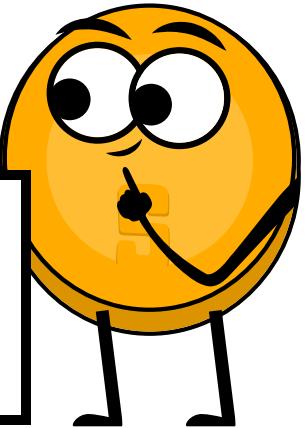
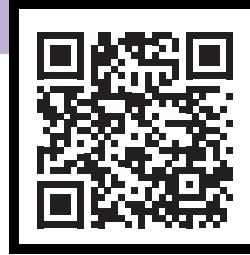


Gracias al sistema UTXO, cada vez que se lleva a cabo una **transacción**, se generan nuevos UTXOs que se graban en la **cadena de bloques**. Esta **cadena de bloques** es accesible para todos en la red y permite rastrear cada **bitcoin** desde el momento en que fue minado por primera vez hasta su **transacción** más reciente. Esta transparencia es fundamental en el sistema UTXO y ayuda a mantener la seguridad e integridad de **Bitcoin**.

### 7.5.1 Ejercicio de Clase: Explorando Transacciones No Confirmadas en Bitcoin: Una Guía para Entender la Mempool y la Tarifa de Transacción

*Ejercicio de Clase.* Siga las siguientes instrucciones:

1. Visita el sitio web:  
<https://bits.monospace.live/> y <https://mempool.space/>
2. Localiza una **transacción** no confirmada y haz clic en ella.
  - ¿Qué información puedes encontrar?
  - ¿Puedes seguir el historial de dónde vino el **bitcoin**? ¿Hay alguna **dirección** conocida o notable en la cadena de **transacciones**?
  - ¿Cuántas **direcciones** ves? ¿Qué significa entrada y salida?
  - ¿Puedes seguir el UTXO? ¿Reconoces cuál **BTC** ha sido gastado y cuál sigue siendo no gastado?
  - ¿Coincide la entrada con la salida? ¿Hay algún cambio sobrante que se envió a una nueva **dirección**?
  - ¿Todas las **transacciones** tienen una tarifa? ¿Cómo se calcula la tarifa?
  - ¿A quién va la tarifa? ¿Es justa? ¿Qué pasaría si no hubiera tarifa o si la tarifa fuera muy baja?
  - ¿Quién paga la tarifa? ¿Es el remitente o el receptor?
  - ¿Puedes encontrar cuánto **BTC** se transfirió de una **dirección** a otra? ¿Cuánto **BTC** se gastó en la **transacción** ?
3. Escribe el TxID, la tasa de tarifa, la tarifa y el valor total de la **transacción** en un cuaderno.
4. Analiza otras **transacciones** si lo deseas y compáralas con la primera en términos de cantidad, tarifa pagada y probabilidad de ser incluida en el próximo bloque.
5. Considera lo que significa que se "mine" un bloque y que una **transacción** esté "no confirmada". ¿Qué factores influyen en la velocidad a la que una **transacción** es confirmada?
6. Prepárate para discutir estas observaciones y preguntas en la próxima clase.





# Capítulo #8

## Construyendo la Cadena de Seguridad: Entendiendo el Proceso de Minería

8.0 Una Introducción a la Minería de **Bitcoin**

8.1 La Estructura de Incentivos en Minería

    8.1.1 El Sistema de Recompensa de Bloques  
        y su Origen

    8.1.2 El Concepto de “Halving”

    8.1.3 La Evolución y La Importancia de los “Pools”  
        de Minería

8.2 Cadena Inquebrantable: La Dinámica del Hash  
    de Bloque.

    8.2.1 El Hash del Bloque y el Valor Objetivo

8.3 Candidatos a Bloque: Tejiendo Historias Épicas.

    8.3.1 Estructurado de un Bloque

    8.3.2 **Transacción Coinbase**

8.4 La Búsqueda del Hash Válido.

8.5 La Gran Carrera del Hash.

    8.5.1 Actividad Interactiva de Minería

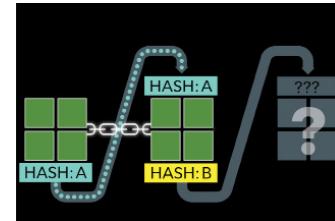
    8.5.2 Actividad. Proceso de Transacciones y  
        Minería en el Modelo UTXO

# Construyendo la Cadena de Seguridad

## 8.0: Una Introducción a la Minería de Bitcoin: Una Analogía

### Las Reglas

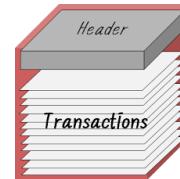
Imagina **Bitcoin** como un libro de historia siempre en crecimiento. Cada **transacción** es una nueva oración, escrita con tinta ineditable. Cada capítulo en este libro (que podríamos llamar bloque) tiene un "título" único. Este título es un código especial (conocido como hash) que resume todo lo que hay en ese capítulo. Si cambias aunque sea una letra del capítulo, este "título" se altera y todos se dan cuenta al instante.



### Validación de la Historia:

Para avanzar a la siguiente página del libro, es necesario que un grupo de verificadores la apruebe. Cuando un escritor, que en el mundo de **Bitcoin** llamamos minero, piensa que ha creado la próxima página perfecta, la presenta para revisión. Los verificadores (otros mineros) se aseguran de que la nueva página empiece con el "título" de la página anterior. Es como tener el número de la página anterior en la nueva, pero más seguro. Si todo encaja, la nueva página se añade al libro. Si algo no cuadra, se descarta y el escritor debe intentarlo de nuevo.

La **cabecera** es donde se encuentra el **hash del bloque** y el **hash del bloque anterior**



### Ganando por Trabajar

El trabajo de escribir no es solo por amor al arte; los escritores son recompensados por su labor. Cada vez que uno de ellos logra añadir una página al libro, recibe "monedas de oro", que en nuestro mundo representan **BTC**. Las "monedas de plata" que a veces reciben simbolizan las tarifas que se pagan por dar prioridad a ciertas **transacciones** o historias..

### Trabajar para Ganar

Con tantos escritores intentando añadir sus páginas, se podría pensar que el libro se llenaría rápidamente. Pero, en realidad, conseguir que una página sea aceptada es un desafío. Los escritores deben esforzarse continuamente para superar a sus pares y lograr que su página sea la elegida.





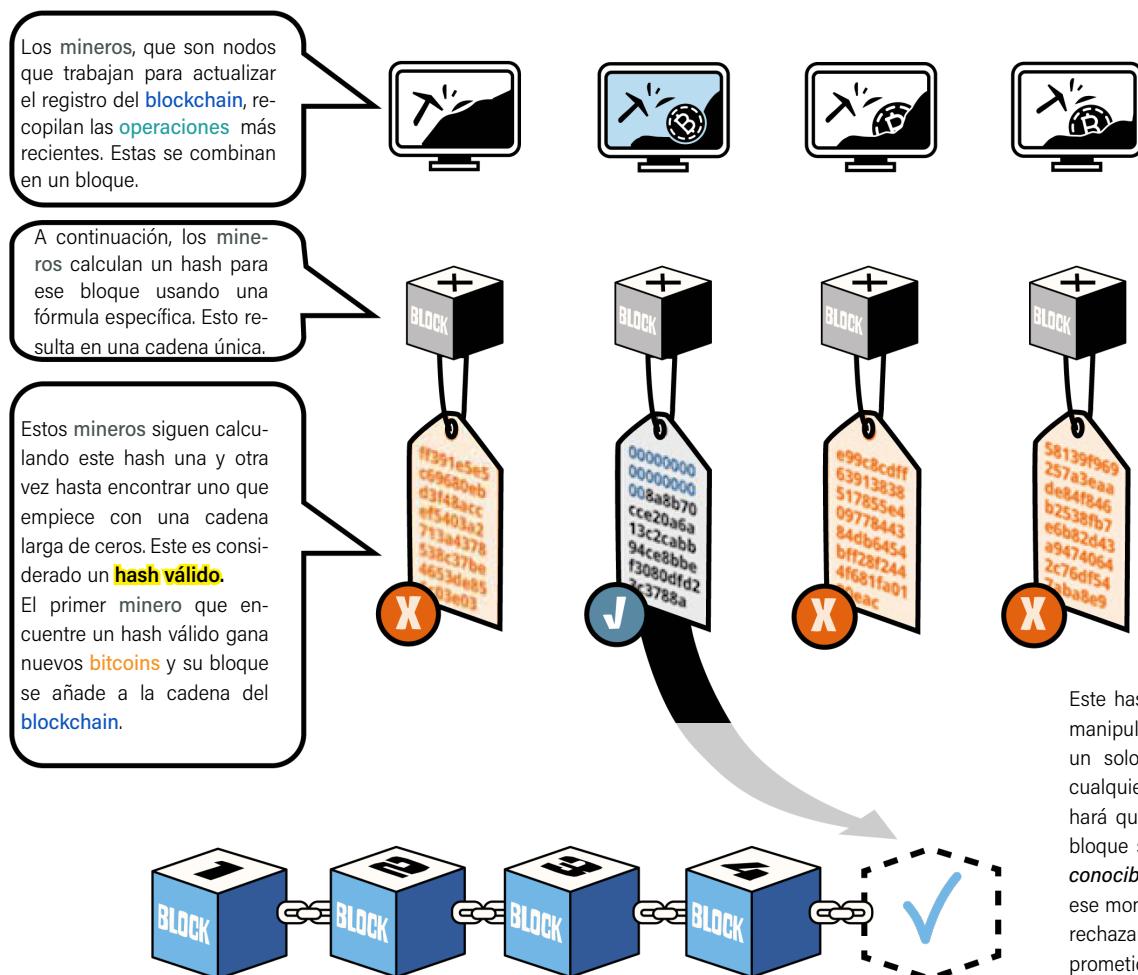
## Capítulo #8

### El Equilibrio

Para garantizar que el libro no se complete demasiado rápido y para mantener a todos los escritores en igualdad de condiciones, hay un equilibrio. Si muchos escritores comienzan a tener éxito en sus envíos, las "reglas del libro" se adaptan, haciendo que la tarea de escribir una página perfecta sea más desafiante. Este equilibrio refleja la forma en que la **dificultad** de la minería de **Bitcoin** se ajusta a lo largo del tiempo, garantizando que no se agreguen bloques demasiado rápido a la cadena.

### El Tesoro Final

Este libro en constante desarrollo es un tesoro en sí mismo. Cada página anexada aumenta su valor. Y aunque todos pueden leer y verificar las páginas anteriores, la belleza radica en que es prácticamente imposible alterar las páginas una vez que han sido añadidas. Es un testimonio de la seguridad y la transparencia, características centrales de **Bitcoin**.



# Construyendo la Cadena de Seguridad

## 8.1. La Estructura de Incentivos en Minería. Un Vistazo al ¿Por qué?

### 8.1.1 El sistema de recompensa de bloques y su origen

El funcionamiento eficaz de la red **Bitcoin** requiere esfuerzo y recursos. Este principio fue bien entendido por Satoshi Nakamoto, el creador de **Bitcoin**. Comprendió que para mantener una red descentralizada y segura, es esencial motivar a los mineros a invertir su tiempo, esfuerzo y recursos. ¿Pero qué implicaciones tiene esto realmente para un minero?



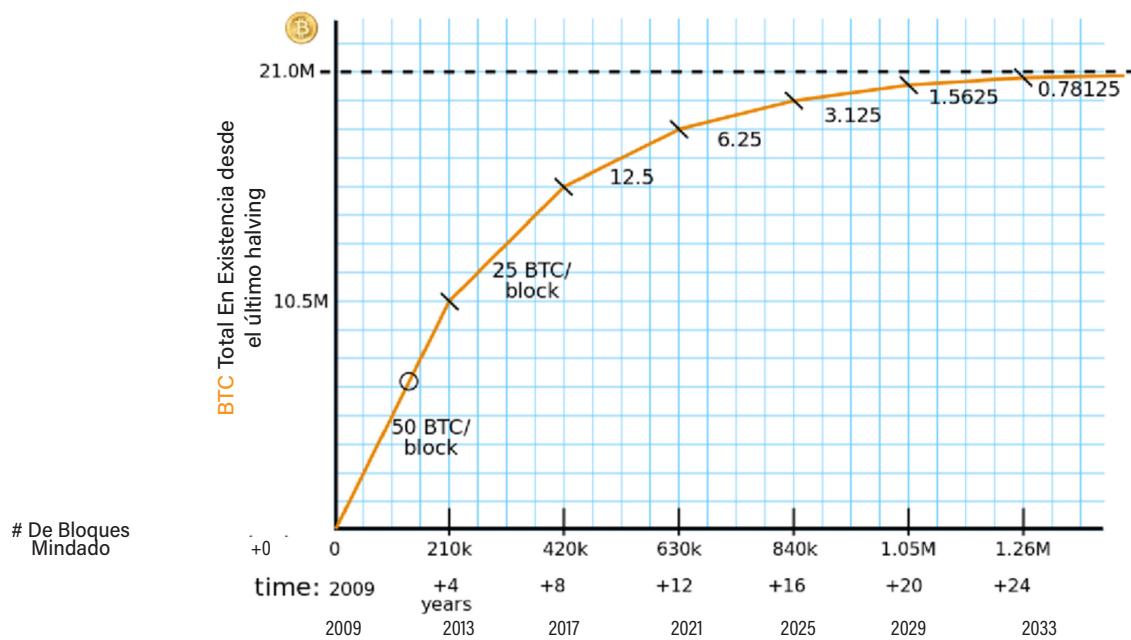
¿Cuál realmente es el trabajo de un minero?

El primer bloque lo minó Satoshi Nakamoto (llamado el bloque Génesis). Como recompensa por su trabajo, el protocolo de **Bitcoin** le concedió un total de 50 **BTC**.



1. Verificar las **transacciones**, lo que implica comprobar que las partes implicadas tienen fondos suficientes y que las firmas y **transacciones** son legítimas.
2. Asegurar la red al agregar las **transacciones** a la **cadena de bloques**, que una vez integradas, no pueden alterarse sin el consenso de la mayoría.

### Recompensa a los Mineros por Completar un Bloque con Éxito a Través del Tiempo



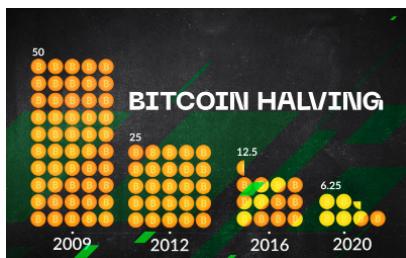


## Capítulo #8

### 8.1.2 El concepto de "halving"



Para preservar la estabilidad de la red **Bitcoin** a largo plazo, es vital regular la velocidad a la que se generan nuevos **bitcoins**. Esto se logra a través del "halving". Cada 210,000 bloques, que equivale a unos cuatro años, la recompensa que los mineros reciben por bloque minado se reduce a la mitad. Este mecanismo desacelera la creación de nuevos **bitcoins**, asegurando que la cantidad total de **bitcoins** nunca superará los 21 millones. Actualmente, los mineros reciben 6.25 **bitcoins** por cada bloque que añaden a la **cadena de bloques**. Esta cantidad seguirá disminuyendo con cada evento de "halving" futuro.



Evento	Fecha Esperada	Bloque	Recompensa de Bloque	Porcentaje Minado
Cuarto Halving	2024	840,000	3.125	96.875 %
Quinto Halving	2028	1,050,000	1.5625	98.4375 %
Sexto Halving	2032	1,260,000	0.78125	99.21875 %



### La estrategia de emisión de Bitcoin

Esta estrategia es un plan diseñado para la creación y liberación de nuevos **bitcoins** en circulación, manteniendo la escasez de **bitcoin** a lo largo del tiempo. La disminución en la emisión de nuevos **bitcoins**, combinada con una demanda creciente, puede llevar a un aumento en el precio de **bitcoin**. Este fenómeno beneficia a los primeros adoptantes de la tecnología y también incentiva a los mineros a seguir protegiendo la red y aportando su poder computacional y recursos.

# Construyendo la Cadena de Seguridad

## 8.1.3 La Evolución y la Importancia de los "Pools" de Minería

La minería de **Bitcoin** ha experimentado grandes cambios desde su inicio. Comenzó con la minería en las unidades de procesamiento central (CPU) de computadoras personales, luego se avanzó a las unidades de procesamiento gráfico (GPU) más potentes y finalmente se llegó a los circuitos integrados de aplicación específica (ASIC), dispositivos dedicados para la minería de **Bitcoin**. La rentabilidad de la minería depende de varios factores como el costo de la maquinaria y de la energía.



Los mineros reciben recompensas en **bitcoin** por cada nuevo bloque de **transacciones** válidas que crean, y esto constituye el retorno de la inversión.

Con el paso del tiempo y el incremento en la dificultad de la minería, la actividad ha pasado de ser un esfuerzo individual a la formación de "piscinas de minería". En estas "piscinas", los mineros agrupan sus recursos para aumentar sus posibilidades de obtener recompensas. Al unirse a un "pool", los mineros contribuyen con su poder de cómputo al grupo y comparten las recompensas en función de su contribución.

Esta estrategia se ha vuelto cada vez más relevante, ya que mejora la eficiencia de la minería y permite a los mineros mantenerse competitivos en un entorno cada vez más desafiante. Es importante considerar factores como las tarifas del "pool", el software utilizado y la reputación del "pool" al elegir uno para unirse. Esto les permite obtener ingresos más regulares y estables en comparación con la minería en solitario.

La decisión de minar en solitario o en un pool depende de las preferencias individuales, los recursos disponibles y la tolerancia al riesgo del minero. A la derecha podemos ver las ventajas y desventajas de ambas opciones.

### Dato interesante:

El 1 de mayo de 2020, algo raro pasó en la minería de Bitcoin. Normalmente, se crean 6 nuevos bloques cada hora. Pero ese día, se hicieron 16 bloques en solo una hora. Los bloques se hicieron muy rápido, con solo 46 segundos entre cada uno. Esto es inusual porque no hay un horario fijo para crear nuevos bloques. A veces puede tardar mucho tiempo, como la vez que pasaron 25 horas para hacer solo un bloque nuevo.

	Minería en solitario	Minería en pool
Ventajas		
Control total	✓	✗
Recompensas completas	✓	✗
Mayores probabilidades de éxito	✗	✓
Ingresos más predecibles	✗	✓
Soporte y comunidad	✗	✓
Desventajas		
Dificultad alta	✓	✗
Ingresos impredecibles	✓	✗
Costos altos	✓	✗
Recompensas divididas	✗	✓
Tarifas del pool	✗	✓
Menos control	✗	✓



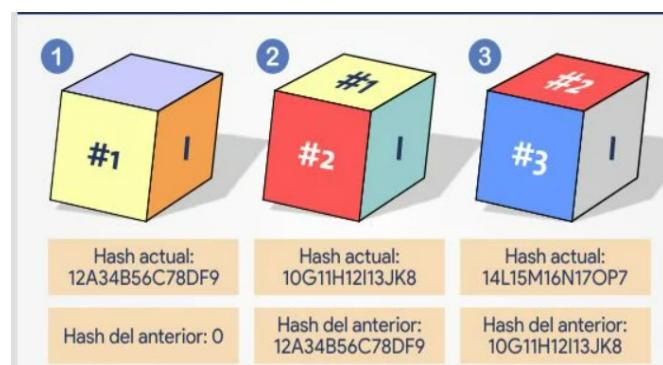
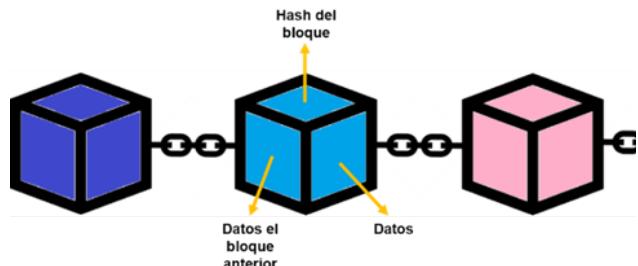
## Capítulo #8

### 8.2 Cadena Inquebrantable: La Dinámica del Hash de Bloque. Un Vistazo al ¿Qué?

Cada bloque en la **blockchain** tiene un hash único, que actúa como su huella digital. Esta cadena de caracteres única cambia con cada pequeña modificación en el bloque, haciendo prácticamente imposible alterar la información sin ser detectado.

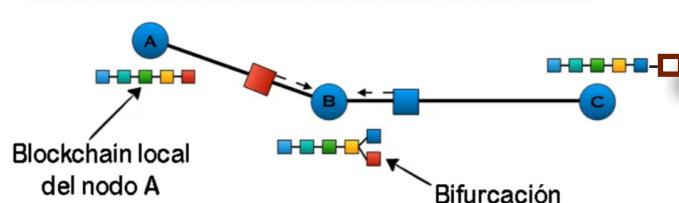
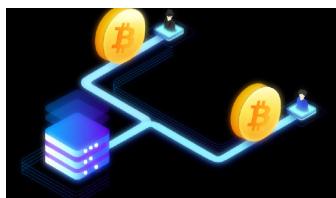
Al igual que un libro con páginas encadenadas, cada bloque en la **blockchain** se enlaza al siguiente, creando una secuencia desde el primer bloque hasta el más reciente. Cada bloque almacena un grupo de **transacciones**, conformando un registro público y transparente.

Los mineros de **Bitcoin** son esenciales en este proceso. Su trabajo consiste en descubrir el hash correcto para un bloque, lo que valida las **transacciones** y añade un nuevo bloque a la cadena.



Existen casos en los que dos mineros pueden encontrar un hash válido para un bloque casi simultáneamente, creando dos versiones posibles de la **cadena de bloques**, a esto se le llama una bifurcación.

Imaginemos cuatro mineros: Eliana, Natalia, Andrés y Juan Diego. Todos están buscando el hash correcto para el próximo bloque, el Bloque 101. Eliana y Natalia encuentran un hash válido para este bloque casi al mismo tiempo, creando una bifurcación. Andrés sigue la versión de **Eliana** y Juan Diego sigue la de **Natalia**.



Si Andrés consigue hallar el hash válido para el **Bloque 102** antes que los demás y lo comunica a la red, la cadena que incluye su bloque se vuelve la dominante, dado que es la más larga. Esta es una de las reglas fundamentales del protocolo de **Bitcoin**: la cadena más larga se considera la válida. Por lo tanto, todos los mineros, incluyendo a Juan Diego, dejan de lado la versión del Bloque 101 de Natalia y se enfocan en el Bloque 103, utilizando como base la cadena más larga, que ahora incluye la versión del **Bloque 101** de Eliana y el **Bloque 102** de Andrés. De esta manera, se soluciona la bifurcación en la red. Esto es consenso!!

# Construyendo la Cadena de Seguridad

## 8.2.1 El Hash del Bloque y el Valor Objetivo

### Minería de Bloques: Un Juego de Dados

Imagina que la minería de **Bitcoin** es como jugar un juego de dados muy especial. En este juego, el objetivo no es lanzar el dado para obtener un número alto, sino más bien lanzar para obtener un número cuya suma sea menor o igual a una cierta cantidad, digamos 120. Esa cantidad es lo que llamamos el "valor objetivo".



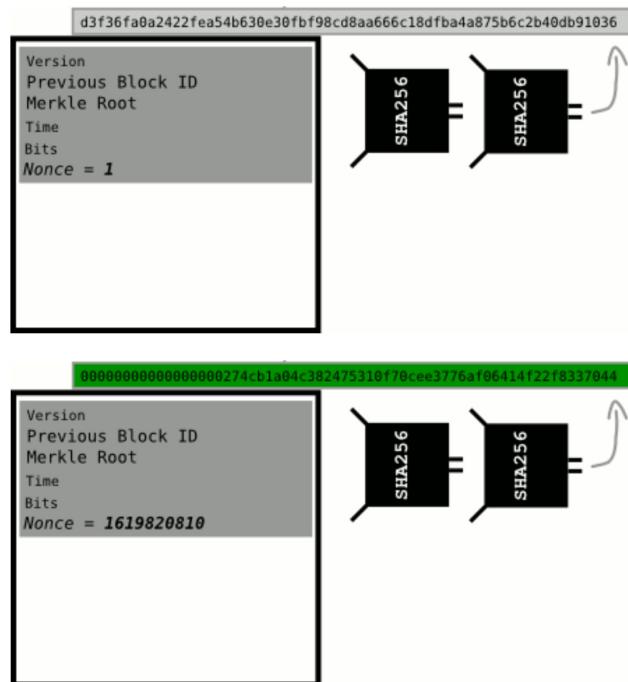
Cada lanzamiento de los dados es un intento de los mineros por resolver un problema matemático difícil, y al igual que en cualquier juego de dados, no puedes simplemente decidir el número que sale cuando lanza los dados, debes probar una y otra vez hasta obtener el resultado deseado.

Pero hay un giro. En este juego, la cantidad objetivo (40 en nuestro ejemplo) puede cambiar con el tiempo. Algunas veces el juego se vuelve más fácil y otras veces se vuelve más difícil. Eso es lo que llamamos la "dificultad de la minería" y es un reflejo de cuánta competencia hay en la **red de Bitcoin**.



Al encontrar un **hash de bloque válido**, un minero **demuestra que ha realizado el trabajo requerido** para añadir el nuevo bloque a la **cadena de bloques** y recibir un pago en **bitcoin** por su esfuerzo.

Por lo tanto, para simplificar, podríamos decir que la minería de **Bitcoin** es como un juego de dados en el que los mineros siguen lanzando los dados hasta obtener un número que sea igual o menor que el valor objetivo. El valor objetivo puede ser cualquier número; en nuestro ejemplo, es conseguir un hash que esté por debajo de 17 ceros. Este valor objetivo puede cambiar con el tiempo, lo que ajusta la dificultad del juego. Cuando más mineros compiten en la red, el juego se vuelve más difícil y viceversa. De esta manera, el "juego" se mantiene competitivo y justo para todos los mineros, independientemente de cuántos estén participando en un momento dado.





## Capítulo #8

La **Prueba de Trabajo** (PoW, por sus siglas en inglés) es una clave para la seguridad de la **blockchain**. Su función es evitar que individuos malintencionados se apoderen de la red. De forma simple, el PoW ajusta la dificultad de minar bloques a un ritmo constante, aproximadamente cada 10 minutos, haciendo que sea cada vez más difícil manipular la red.



En el contexto de la minería en **Bitcoin**, esta se puede equiparar a una competencia de corredores. Cuantos más corredores haya (es decir, mineros), más difícil será ganar. Por eso, los mineros siempre buscan mejorar su equipo para mantenerse en la competencia.



El minero que descubre un hash válido para el bloque antes que los demás, se gana el derecho de añadir el nuevo bloque a la **cadena de bloques** y, además, recibe una recompensa monetaria en forma de **bitcoin**. Este proceso de competencia no solo impulsa la minería, sino que también asegura la integridad de la cadena. Un atacante que intente alterar un solo carácter en una **transacción** provocaría que las verificaciones de bloques subsiguientes fallen, preservando así la seguridad y la precisión de los datos almacenados en la red.



SHA-256

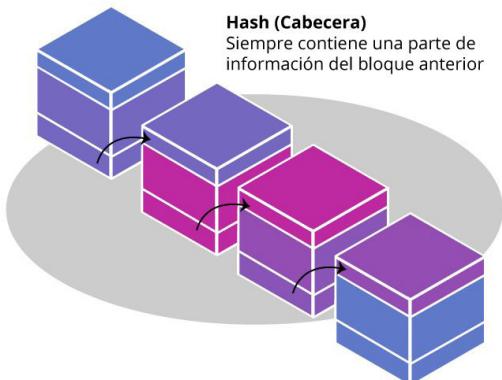
10101010101001010
10101010101001010
10101010101010100
10101010101010101
00101010101010101
001010101010101010

SHA-256

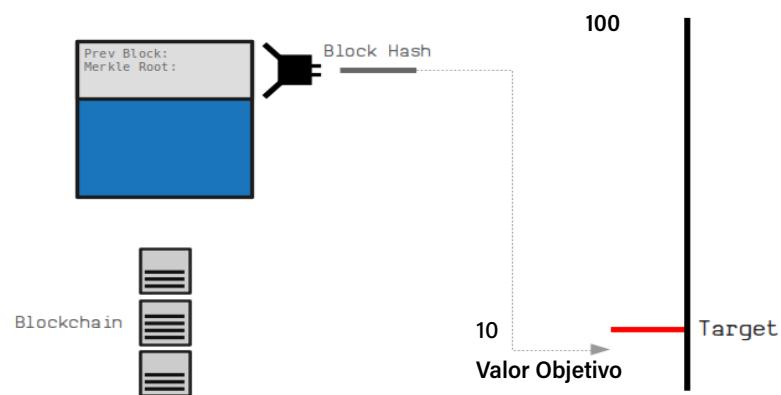
000000000010010
10101010101010010
10101010101010101
00101010101010101
01001010101010101
010010101010101010

SHA-256

10101010101001010
10101010101001010
10101010101010100
10101010101010101
00101010101010101
001010101010101010



Este proceso de competencia asegura la integridad de la cadena. Un atacante que intente alterar un solo carácter en una **transacción** provocaría que las verificaciones de bloques subsiguientes fallen, preservando así la seguridad y la precisión de los datos almacenados en la red.



# Construyendo la Cadena de Seguridad

## 8.3 Candidatos a Bloque: Tejiendo Historias Épicas. Explorando el ¿Cómo?

En el vasto universo de la minería de **Bitcoin**, un concepto esencial para comprender cómo se añaden nuevos bloques a la cadena es el de los bloques candidatos.



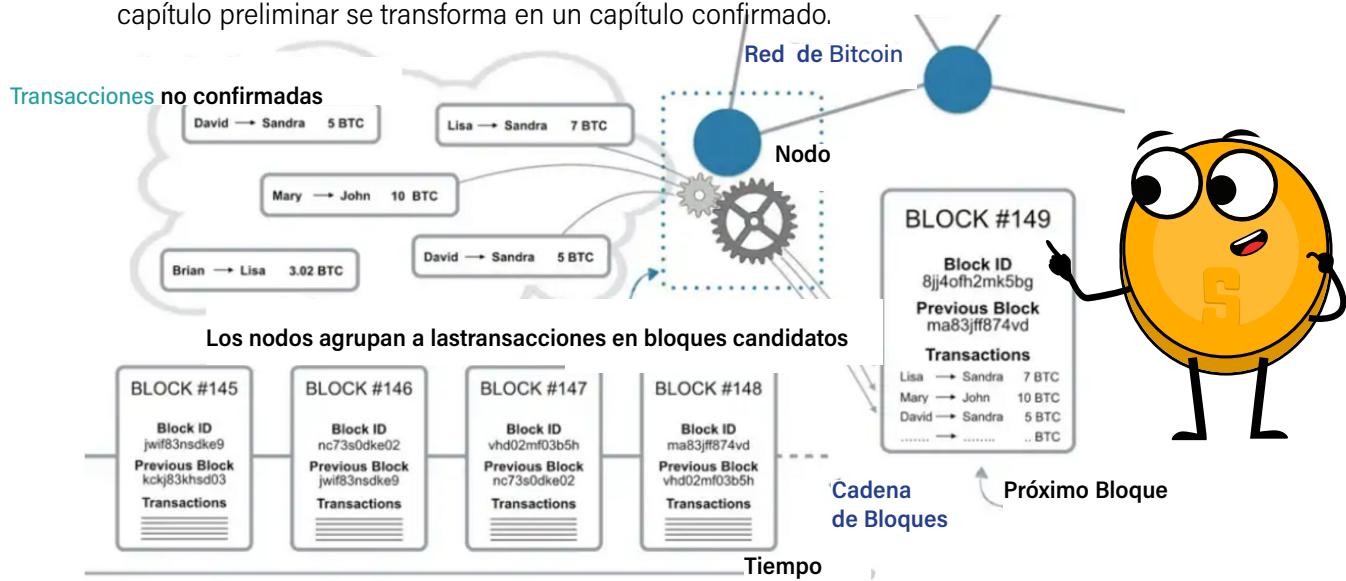
Un **bloque candidato** es un bloque de **transacciones** que se está considerando para agregar a la **cadena de bloques** pero aún no se ha agregado.

Retomando nuestra analogía del Gran Libro de Historia, un bloque candidato es semejante a un borrador de capítulo que un escritor propone para la saga en curso. Estos borradores, aunque llenos de potencial, aún no han sido incorporados en el relato principal; todavía no han sido reconocidos por la comunidad literaria. Aquí está el proceso que sigue un escritor (minero):

**Selección de eventos:** Los escritores recogen acontecimientos y hechos (**transacciones** no confirmadas) que surgen en su imaginación (mempool) y eligen aquellos que creen que aportarán un giro interesante al relato.

**Creación de un capítulo preliminar:** Con estos eventos, los escritores elaboran un borrador que se adapta a la trama ya establecida en el **Gran Libro de Historia**.

**Búsqueda del título adecuado:** Los escritores buscan el título perfecto para su capítulo, que resuma y represente adecuadamente su contenido (hash de bloque válido). Si un escritor encuentra un título que se ajusta perfectamente, lo comparte con el resto de escritores. Si la comunidad literaria coincide en que el título y el contenido son coherentes y relevantes, el capítulo (bloque) se incorpora oficialmente al Gran Libro de Historia. En este momento, el capítulo preliminar se transforma en un capítulo confirmado.





## Capítulo #8

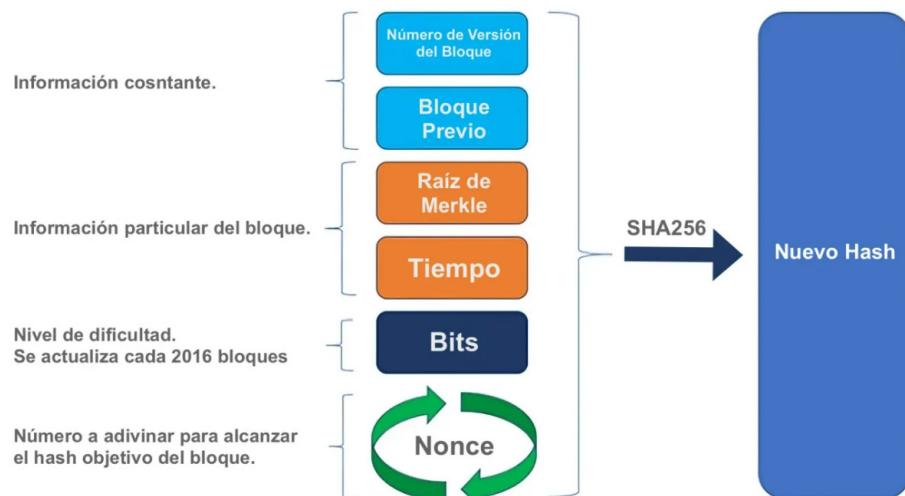
**4. Verificación y adición del bloque:** Si un buscador logra formar una palabra válida, la anuncia a los demás. Si los otros buscadores están de acuerdo en que la palabra es válida, la palabra (bloque) se añade oficialmente a la historia ([cadena de bloques](#)). En este punto, el bloque candidato se convierte en un bloque confirmado.

### La Búsqueda del Nonce: Encontrando la Palabra Perdida en el Gran Libro de Historia

En nuestro gran libro de historia, los escritores, que simulan a los mineros de [Bitcoin](#), han compilado una serie de eventos y están a punto de completar una página. Sin embargo, les falta un detalle crucial: la "palabra perdida". Esta palabra, cuando se añade a la narración, le otorga a toda la página un significado especial y único.

Estos escritores, con sus páginas casi completas, se embarcan en una tarea desafiantes. Compiten para probar millones, incluso billones, de posibles "palabras perdidas", con la esperanza de ser los primeros en descubrir la correcta. Es un esfuerzo meticuloso, una carrera de ingenio y perseverancia.

Esta metáfora es análoga a cómo los mineros de [Bitcoin](#) buscan el **nonce**, o "Número usado una sola vez". En [Bitcoin](#), este nonce es un número que, cuando se añade a un bloque candidato (un conjunto de [transacciones](#) que aún no ha sido verificado) y se realiza un hash en conjunto con el resto del bloque, si el resultado satisface el **valor objetivo**(o **el target**), el bloque candidato se convierte en un bloque confirmado y se añade a la [cadena de bloques](#).



El proceso de hallar este nonce se asemeja a la búsqueda de la "palabra perdida" en el Gran Libro de Historia: demanda una gran cantidad de esfuerzo y consume vastos recursos. En ambos contextos, la recompensa para quien lo logra es significativa. En el Gran Libro de Historia, el escritor es aclamado y gana más reconocimiento; en [Bitcoin](#), el minero obtiene [bitcoins](#) y las tarifas de [transacción](#) del bloque recién minado.



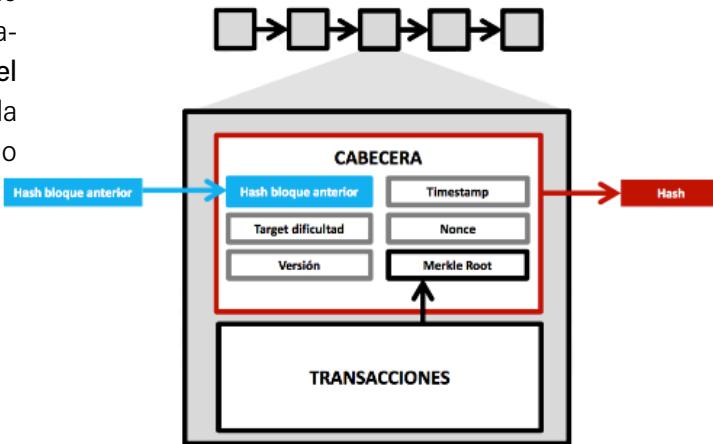
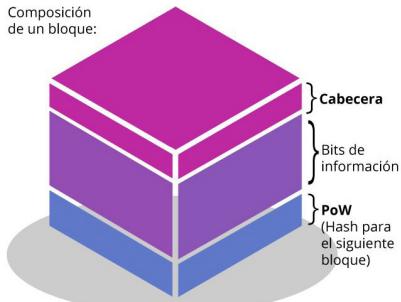
¡El proceso de encontrar el *valor de hash* correcto cambiando el **nonce** se llama minería!



# Construyendo la Cadena de Seguridad

## 8.3.1 El Estructurado de un Bloque: Anatomía de un Elemento Vital

Cada bloque dentro de la **cadena de bloques** de **Bitcoin** está compuesto por tres partes principales: la **cabecera**, las **transacciones** y el **hash del bloque anterior**. Para entender cómo funciona la **cadena de bloques**, es crucial examinar cada uno de estos componentes y su importancia.



### Hash del Bloque Anterior: Un Eslabón Fuerte en la Cadena de Historias

El hash del bloque anterior es uno de los componentes clave de un bloque de **Bitcoin**. Su propósito es mantener la conexión entre los bloques y garantizar la cronología de las **transacciones**.

Imagina una cadena de eventos en una historia; cada evento lleva a otro, formando una línea de tiempo lógica. En el caso de la **cadena de bloques** de **Bitcoin**, cada bloque es un capítulo de la historia y el hash del bloque anterior actúa como el enlace entre los capítulos. El hash del bloque anterior está incorporado en la cabecera del bloque actual, lo que en efecto, enlaza cada bloque con el anterior.

Lo fascinante de este diseño es que cualquier intento de alterar un bloque cambiará su hash, y como este hash se ha utilizado en el bloque siguiente, el cambio desencadenará un efecto dominó, rompiendo la conexión entre los bloques. Este mecanismo de "romper la cadena" es lo que mantiene la integridad de la **cadena de bloques** y evita la alteración de **transacciones** pasadas.

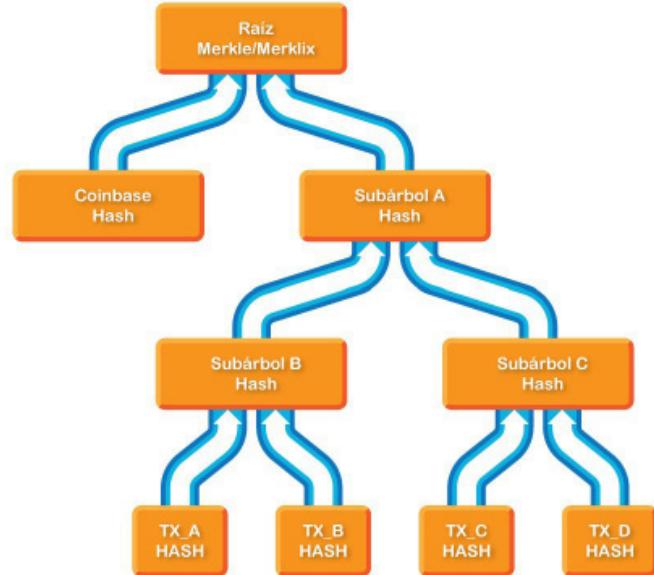
### Las Transacciones y el Árbol de Merkle: Un Bosque de Actividad Económica

Cada bloque de la **cadena de bloques** de **Bitcoin** contiene una lista de **transacciones** que se han realizado en la red. Estas **transacciones** se organizan de una manera particular utilizando una estructura llamada **árbol de Merkle**.



## Capítulo #8

El árbol de Merkle es una estructura de datos en forma de árbol en la que cada hoja es un hash de una **transacción** y cada nodo es un hash de los hashes de sus nodos hijos. Esta estructura permite un almacenamiento eficiente y verificación de las **transacciones** dentro de un bloque. Además, el hash de la raíz del árbol de Merkle, que es un resumen de todas las **transacciones** en el bloque, se incluye en la cabecera del bloque.



### Cabecera del Bloque: El Rostro Identificable de un Bloque

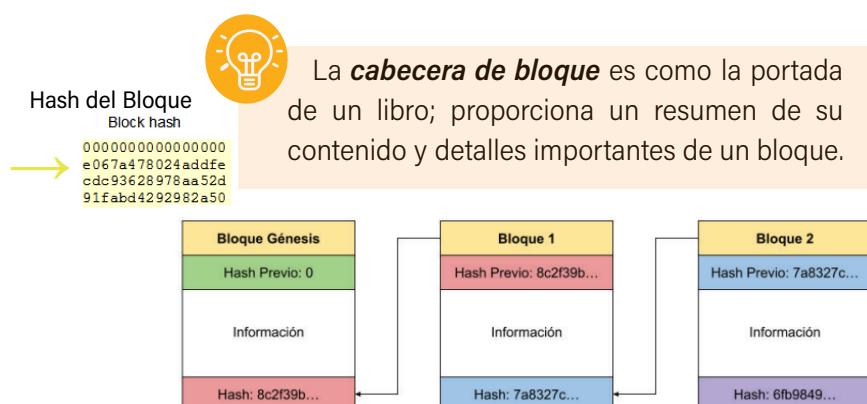
La cabecera de un bloque es esencialmente su "número de identificación", que contiene información que lo identifica y lo conecta con el resto de la **cadena de bloques**. Esto incluye el hash del bloque anterior, el mencionado hash de la raíz del árbol de Merkle de las **transacciones** del bloque, la marca de tiempo de cuándo se creó el bloque, el objetivo de dificultad actual para la minería y el nonce, que es el valor que los mineros tienen que encontrar para crear un bloque válido.



La tarea de los **mineros** es completar correctamente la información de la cabecera al crear bloques candidatos. Al hacerlo, no solo establecen una conexión con el bloque anterior, sino que también preparan el terreno para el próximo bloque en la cadena.

De esta manera, cada bloque se convierte en un eslabón vital en la **cadena de bloques** de **Bitcoin**, preservando la historia de las **transacciones** de **Bitcoin** y garantizando la seguridad e integridad de la red.

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55330edab87803c817010000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	<b>Transacción Coinbase</b>
transaction	
	...



La **cabecera de bloque** es como la portada de un libro; proporciona un resumen de su contenido y detalles importantes de un bloque.

# Construyendo la Cadena de Seguridad



El **bloque minado** es enviado a la red para su verificación, y una vez que es verificado por otros mineros y se llega a un consenso en la red, el bloque se añade a la **cadena de bloques** como el último bloque en la cadena.

**Raíz de Merkle:** *SHA256 (Hash(H(1,2),H(3,4,)), Hash(H(5,6),H(7,8)))*. Este es el resultado de la función hash aplicada a las **transacciones** en el bloque, proporcionando una huella digital única.

**Actualización de UTXO:** Este proceso implica actualizar los UTXOs (Unspent Transaction Outputs) en la **cadena de bloques**, para reflejar las **transacciones** más recientes.

**Tiempo:** Representa el momento aproximado en que se creó el bloque.

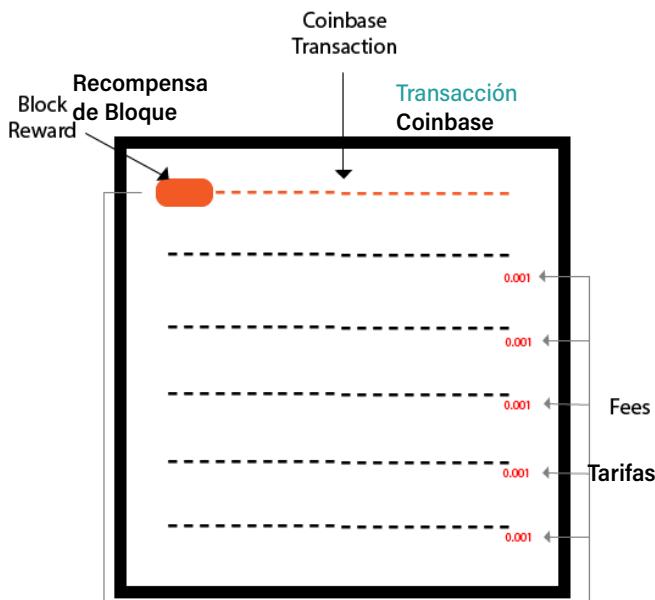
**Bits:** Es el 'objetivo de dificultad' que indica la complejidad requerida para la minería de este bloque. Cuanto mayor sea este valor, más desafiante será para los mineros crear un bloque válido.

**Nonce:** Es un número único que los mineros deben encontrar para crear un bloque nuevo y válido. El proceso de encontrar este número es la esencia de la minería de **Bitcoin**.

## 8.3.2 La Transacción Coinbase: Un Premio Especial en la Cadena de Bloques

La **transacción Coinbase** es única en cada bloque de la **cadena de bloques** de **Bitcoin**. No solo es el mecanismo a través del cual se crean nuevos **bitcoins (recompensa de bloque)**, sino que también permite a los mineros recolectar las tarifas de **transacción** asociadas con las **transacciones** que han incluido en su bloque.

Lo que distingue a la **transacción Coinbase** de otras **transacciones** en la red **Bitcoin** es que no tiene entradas, dado que no proviene de **bitcoins** existentes. En cambio, está generando nuevos **bitcoins** desde cero. Por lo tanto, solo tiene una salida, creando una nueva salida de **transacción** no gastada (UTXO).



La recompensa de los mineros, consistente en nuevos **bitcoins** y tarifas de **transacción**, incentiva a los mineros a mantener la red. Es su paga por el esfuerzo y los recursos que invierten en el proceso de minería. A medida que la cantidad de **bitcoins** que se pueden minar se acerca a su límite de 21 millones, la recompensa en nuevos **bitcoins** disminuirá y eventualmente se detendrá.

Cuando llegue ese momento y todos los **bitcoins** estén minados, las tarifas de **transacción** se convertirán en la única compensación que los mineros recibirán. Esta es la razón por la cual la **transacción Coinbase** es tan esencial en el funcionamiento de la **cadena de bloques** de **Bitcoin**. Permite que la red continúe operando y siendo segura incluso después de que se hayan minado todos los **bitcoins**.

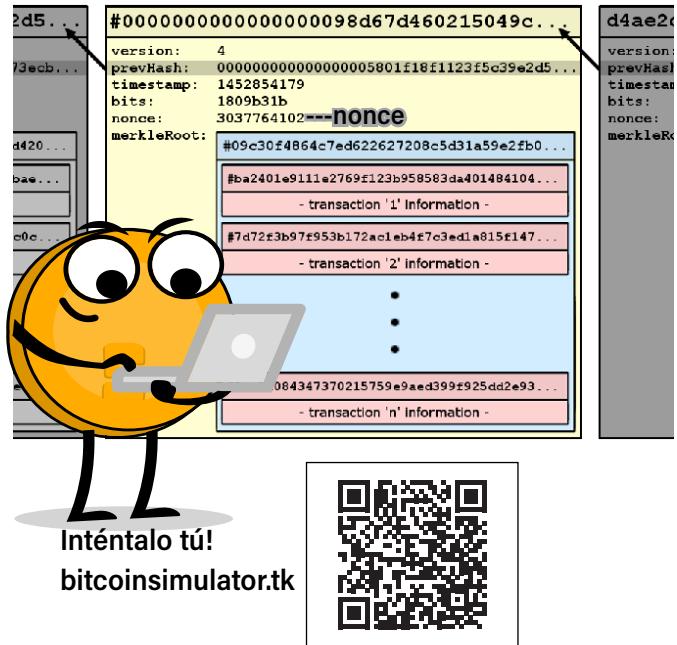


## Capítulo #8

### 8.4 La Búsqueda del Hash Válido: Un Segundo Vistazo al ¿Cómo?

#### Proceso de Cálculo de Nonce

Imagínate que un minero comienza a calcular desde uno y, en cada paso, incrementa el número con el que está trabajando. En nuestro ejemplo, necesitó realizar más de tres mil millones de cálculos para encontrar un valor hash que cumpliera con las normas de la red. Cada cálculo es una búsqueda de un **nonce** que, cuando se añade al bloque en proceso y se aplica el algoritmo de hash, genera un hash de bloque válido. Al descubrir el nonce correcto, el minero consigue agregar un nuevo bloque a la **cadena de bloques**, fortaleciendo la seguridad e integridad de la red.



#### La Influencia de la Tasa de Hash en la Minería

La tasa de hash refleja el poder de cálculo de la **red de Bitcoin**. Podemos compararlo con la cantidad de boletos de lotería que un minero puede comprar: cuantos más boletos adquiere (mayor tasa de hash), mayores son sus posibilidades de ganar (o de minar un bloque). Los mineros pueden aumentar sus posibilidades adquiriendo equipos de cómputo más potentes.

#### Velocidad del bitcoin hashes:

##### 1.1 Exahash / second

- Un hash / segundo
- Un **Kilohash** = 1,000 hashes
- Un **Megahash** = 1,000,000 hashes
- Un **Gigahash** = 1,000,000,000 hashes
- Un **Terahash** = 1,000,000,000,000 hashes
- Un **Petahash** = 1,000,000,000,000,000 hashes
- Un **Exahash** = 1,000,000,000,000,000,000 hashes

#### La Dificultad en la Minería de Bitcoin

Conforme aumenta la tasa de hash de la red, también lo hace la dificultad para minar nuevos **bitcoins**. Para seguir siendo competitivos, los mineros deben actualizar constantemente su equipo y mejorar su tasa de hash.

La dificultad de la minería de **Bitcoin** se ajusta automáticamente cada 2016 bloques (aproximadamente cada dos semanas) para mantener el tiempo de minería de cada bloque cerca de 10 minutos.

# Construyendo la Cadena de Seguridad

Gráfico de dificultad Bitcoin



Si los últimos 2016 bloques se minaron en menos de 14 días, la minería se considera "demasiado fácil" o "rápida", por lo que la dificultad se incrementa. Por el contrario, si los últimos 2016 bloques tardaron más de 14 días en minarse, la minería se considera "demasiado difícil" o "lenta", por lo que la dificultad disminuirá.

## Ajustes en la Dificultad de Minería

Este autoajuste de la dificultad asegura una emisión constante de nuevos **bitcoins** y preserva la seguridad de la red, independientemente del total de potencia de hash (la cantidad total de cálculos que los mineros están haciendo en la red).

Así, la dificultad en la minería de **bitcoin** se ajusta regularmente con base en una fórmula que considera el tiempo promedio que se tardó en minar los 2016 bloques anteriores, garantizando que, independientemente de cuánto poder de hash de minería se aplique, el bloque promedio se mina cada 10 minutos.



No importa cuánto poder de hash de minería se aplique, el bloque promedio se mina cada 10 minutos.

## Aspectos Económicos de la Minería de **Bitcoin**

La minería de **Bitcoin** presenta una serie de desafíos y consideraciones económicas. Uno de los aspectos más importantes es el costo de la electricidad. Dado que la minería de **bitcoin** requiere una gran cantidad de energía, los mineros buscan ubicaciones donde los costos de electricidad sean bajos para maximizar sus ganancias.

Además, la minería de **bitcoin** también requiere una inversión inicial significativa en hardware de minería, especialmente para aquellos que optan por los ASICs más eficientes. La depreciación de este equipo es un factor a considerar, ya que la aparición constante de hardware de minería más potente y eficiente puede reducir rápidamente el valor del hardware existente.

La recompensa de bloque también es una consideración económica crítica en la minería de **Bitcoin**. Cada 210,000 bloques, aproximadamente cada cuatro años, la recompensa por bloque se reduce a la mitad. Este proceso de halving puede tener un impacto significativo en la rentabilidad de la minería, ya que reduce la cantidad de **bitcoin** nuevo que los mineros reciben por su trabajo.



## Capítulo #8

Finalmente, las tarifas de **transacción** también son un factor importante. A medida que la recompensa del bloque disminuye con el tiempo, se espera que las tarifas de **transacción** se conviertan en una proporción cada vez más significativa de las ganancias de los mineros.

Cada uno de estos factores económicos juega un papel en la decisión de un minero de participar en la minería de **Bitcoin** y cómo configurar sus operaciones de minería.



### 8.5. Simulaciones y Ejercicios de Clase

**Ejercicios de Clase.** Siga las siguientes instrucciones:

#### 8.5.1 Ejercicio Interactivo de Minería

1. Accede al siguiente sitio web:

<https://mempool.space/>

2. Revisa los diferentes elementos que se muestran en la página, incluyendo los bloques más recientes, **transacciones** confirmadas, el número de **transacciones**, el uso de memoria y el valor aproximado del bloque completo

Responde las siguientes preguntas:

- ¿Cuál fue el último bloque minado?
- ¿Cuántas **transacciones** se incluyeron ?
- ¿Cuál es el valor total negociado en **bitcoin**?
- ¿Cuál fue el tamaño en megabytes del bloque?
- ¿Cuántos ceros tiene el nonce del bloque?
- ¿Cuánto ganó el minero en total?
- ¿Cuál fue el valor total de las comisiones recibidas por el minero por agregar las **transacciones** a la red?
- Elige una de las **transacciones** de mayor valor en el bloque. ¿A cuántas billeteras de **BTC** se distribuyó la cantidad?



# Construyendo la Cadena de Seguridad

## 8.5.2 Ejercicio: Proceso de Transacciones y Minería en el Modelo UTXO

**Ejercicio de Clase.** Siga las siguientes instrucciones:

**Entiende tu Rol:** Se te asignará uno de los siguientes roles: remitente, receptor, nodo o minero.

- Como **remitente**, serás responsable de crear y transmitir las **transacciones**.
- Como **receptor**, serás responsable de recibir y verificar las **transacciones**.
- Como **nodo**, serás responsable de validar las **transacciones** y seguir las reglas.
- Como **minero**, serás responsable de verificar, agregar las **transacciones** al **blockchain** y recibir recompensas por tu trabajo.

**1. Creación de la Transacción (Remitente):** Utiliza una plantilla de **transacción** y completa los siguientes campos:

- Entrada UTXO: 20 **BTC**
- Salida UTXO: 10 **BTC** a la **dirección** del receptor
- Salida UTXO: 1 **BTC** a la **dirección** del minero
- Cambio UTXO: 9 **BTC** a tu **dirección**
- Firma: Genera tu **firma** usando tu **clave privada**

**2. Verificación de la Transacción (Receptor):** Comprueba que la **transacción** contiene la cantidad correcta de monedas y que la **dirección** de recepción es correcta. Si la **transacción** es válida, marca la aprobación en el gráfico UTXO compartido.

**3. Validación de la Transacción (Nodo):** Verifica que las **direcciones** del remitente y del receptor sean válidas, que el remitente tenga fondos suficientes y que no se dupliquen los gastos.

**4. Minería de la Transacción (Minero):** Verifica las **transacciones** aprobadas por los receptores validadas por los nodos. Lanza los datos y compara los resultados con otros mineros. El minero con el resultado más bajo (menor a 25) agregará la **transacción** al **blockchain** y recibirá una recompensa de 1 **BTC** por su esfuerzo.

**5. Registro de Transacciones (Estudiante):** Mantén un registro de tus monedas durante la actividad.



## Capítulo #8

En este caso, la tabla muestra que la **transacción** inicial se ha gastado, y las **transacciones** 2 a 5 están vacías y listas para ser completadas durante el ejercicio. Recuerda que la Salida UTXO 1 es la cantidad de **BTC** enviada al receptor, la Salida UTXO 2 es la tarifa de la **transacción** enviada al minero, y Cambio UTXO es la cantidad que se devuelve al remitente original.

ID de Transacción	Entrada UTXO (BTC)	Salida UTXO 1 (BTC) (Dirección del receptor)	Salida UTXO 2 (BTC) (Dirección del minero)	Cambio UTXO (BTC)	Balance del remitente (BTC)
-----	-----	-----	-----	-----	-----
-----	-----	-----	-----	-----	-----
Inicial	20	---	---	---	20
1	20	10	1	9	9
2					
3					
4					
5					

**6. Reflexión Final:** Despues de agregar todas las **transacciones** al **blockchain**, discutan en grupo la importancia de la validación, la minería y la creación de nuevos bloques para mantener la integridad y seguridad del **blockchain**.

### 8.6 Diversidad de Direcciones Bitcoin: Por Qué y Para Qué

En el mundo de **Bitcoin**, no todas las **direcciones** son iguales. Existen diferentes tipos de **direcciones**, y cada una tiene sus propias ventajas y desventajas en términos de seguridad, eficiencia y compatibilidad. Algunas **direcciones** son más antiguas y más ampliamente aceptadas, mientras que otras ofrecen mayor seguridad o menores tarifas de **transacción**.

Esta variedad es necesaria porque las necesidades de los usuarios de **Bitcoin** son diversas. Algunas personas priorizan la seguridad por encima de todo, mientras que otras pueden estar más interesadas en minimizar las tarifas de **transacción** o en asegurar la máxima compatibilidad con diferentes servicios y plataformas.

Al ofrecer diferentes tipos de **direcciones**, **Bitcoin** se asegura de que los usuarios puedan elegir la opción que mejor se adapte a sus necesidades y circunstancias particulares. Esto añade flexibilidad y robustez al sistema, haciendo que **Bitcoin** sea aún más útil y resistente. (La pg. 173 muestra los tipos de **direcciones** en detalle).



# Capítulo #9



## Descubriendo el Valor Real de Bitcoin: Más Allá de la Superficie

9.0 ¿Por qué Bitcoin? Una Revolución Financiera y Social

9.1 Desmitificando Bitcoin: Mitos y Realidades

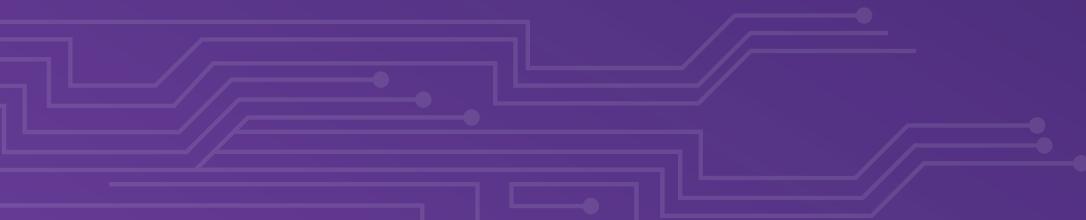
9.2 ¿Qué le da valor al Bitcoin?

9.3 Las Múltiples Dimensiones de Bitcoin

    9.3.1 El Protocolo Base: Bitcoin Core

    9.3.2 Ampliando las Fronteras con la Lightning Network

9.4 Imaginando un Futuro HiperBitcoinizado



# Descubriendo el Valor Real de Bitcoin: Más Allá de la Superficie

## 9.0 ¿Por qué Bitcoin? Una Revolución Financiera y Social

El sistema monetario moderno ha experimentado una transformación drástica. Pasamos de un sistema basado en materias primas, como el oro y la plata, a una economía de dinero fiduciario, respaldada por la fe en el gobierno. Este sistema, sin embargo, presenta múltiples desafíos, entre los que se incluyen la inflación, la devaluación, la deuda excesiva y la desigualdad de riqueza, así como preocupaciones en torno a la privacidad, el control y la censura financiera. La necesidad de una alternativa viable es cada vez más urgente en nuestro mundo digital e interconectado.

En este contexto, surge **Bitcoin**.

**Bitcoin** no solo está cambiando la forma en que pensamos sobre el dinero y la tecnología; también está tejiendo su presencia a través de varios aspectos de la sociedad. Está empoderando a individuos en el área social al ofrecer una alternativa financiera más inclusiva, especialmente en regiones donde los sistemas bancarios tradicionales son inaccesibles o poco confiables. A través de la minería, **Bitcoin** está creando un nuevo modelo económico que premia la contribución de recursos computacionales para mantener la red. En el ámbito tecnológico, su infraestructura descentralizada y su código abierto están impulsando innovaciones que van más allá de las **transacciones** financieras, como contratos inteligentes y aplicaciones descentralizadas.

Este alcance multifacético de **Bitcoin**, que abarca lo social, lo económico y lo tecnológico, lo posiciona como una fuerza transformadora en la sociedad moderna. En lugar de ser solo una moneda digital, se está convirtiendo en una revolución integral que podría abordar algunos de los problemas más arraigados de nuestro sistema financiero actual. Al hacerlo, está allanando el camino para un futuro más equitativo y descentralizado.

## 9.1 Desmitificando Bitcoin: Mitos y Realidades

Es común escuchar muchas ideas erróneas sobre **Bitcoin**, algunas de las cuales pueden confundir a las personas o disuadirles de aprender más. En esta sección, abordaremos algunos de estos mitos y expondremos las realidades para proporcionar un cuadro más claro.



Las posibilidades de cambio positivo son inmensas, por lo que te invitamos a ver este vídeo para obtener más información: "[Bitcoin es Riqueza Generacional](#)"





## Capítulo #9

Algunas personas consideran que Bitcoin es estático y anticuado por varias razones:

- **Desconocimiento:** Muchos aún no entienden completamente la tecnología detrás de Bitcoin y pueden verlo simplemente como una moneda digital sin mucho más que ofrecer.
- **Primera Generación:** Al ser la primera criptomoneda, a menudo se compara con tecnologías más nuevas que ofrecen características adicionales, como contratos inteligentes en Ethereum.
- **Velocidad y Escalabilidad:** Las limitaciones actuales en la velocidad de las transacciones y la escalabilidad de la red pueden llevar a la percepción de que Bitcoin no puede manejar las demandas de una economía global.
- **Medios de Comunicación:** Los informes de los medios a menudo se centran en criptomonedas más nuevas con características técnicas más avanzadas, lo que puede hacer que Bitcoin parezca desactualizado en comparación.
- **Resistencia al Cambio:** El diseño de Bitcoin prioriza la seguridad y la descentralización, lo que significa que cualquier cambio en su protocolo requiere un consenso amplio. Esto puede hacer que el desarrollo parezca lento.
- **Competencia:** La aparición de numerosas criptomonedas y tokens con diferentes casos de uso y características puede hacer que Bitcoin parezca una tecnología más vieja y menos versátil.

Mito	Realidad
<b>Bitcoin Es Anónimo</b>	Aunque <b>Bitcoin</b> ofrece más privacidad que muchos métodos tradicionales de pago no es completamente anónimo. Todas las <b>transacciones</b> se registran en la <b>cadena de bloques</b> que es pública.
<b>Solo Se Usa para Actividades Illegales</b>	<b>Bitcoin</b> se utiliza para una variedad de aplicaciones legítimas como inversiones remesas y compras de bienes y servicios. Su utilidad como una forma de dinero rápido y sin fronteras es universal.
<b>Bitcoin es una Burbuja</b>	Aunque el valor de <b>bitcoin</b> ha experimentado alta volatilidad también ha mostrado un crecimiento y adopción sostenidos desde su creación. No es simplemente una burbuja especulativa sino una tecnología emergente.
<b>La Minería de bitcoin es Malgastar Energía</b>	La minería de <b>bitcoin</b> sí consume energía, pero este consumo debe contextualizarse con los beneficios que aporta y cómo se compara con otros sistemas financieros y de pago. Además, cada vez se utiliza más energía renovable en la minería de <b>bitcoin</b> .
<b>Bitcoin No Tiene Valor Real</b>	<b>Bitcoin</b> posee atributos de un buen dinero: es divisible, duradero, transportable, reconocible y escaso. Su valor se deriva de estos atributos, así como de la confianza y utilidad que las personas le otorgan.
<b>Bitcoin es Inseguro</b>	La tecnología de <b>blockchain</b> de <b>Bitcoin</b> es muy segura y ha resistido pruebas intensas a lo largo de los años. Los riesgos de seguridad suelen estar más asociados con el mal manejo de las <b>claves privadas</b> por parte del usuario que con la propia tecnología.

# Descubriendo el Valor Real de Bitcoin: Más Allá de la Superficie

## 9.2 ¿Qué le da valor a bitcoin?

El valor de bitcoin proviene de varias características únicas:



**Escasez definida:** Al igual que el oro, solo habrá 21 millones de bitcoins. A diferencia del dinero tradicional, no se puede imprimir sin límites.



**Descentralización:** Como moneda digital, opera sin una entidad central. Esto significa autonomía, sin permiso, y resistencia a la censura.



**Valor percibido:** La comunidad global valora a bitcoin como inversión, refugio contra la inflación, y medio de intercambio neutral.



**Inmutabilidad:** Las transacciones en bitcoin son permanentes. Una vez que se confirma, no se puede modificar ni revertir.



**Soberanía y seguridad:** Es virtualmente intocable. Bitcoin es muy seguro y da mucho control a quien lo usa. Es código abierto (cualquiera puede ver cómo funciona), y es muy difícil confiscar. Por lo tanto, es atractivo para aquellos que buscan libertad financiera y protección contra intrusiones indeseadas.



**Oferta y Demanda:** El valor de bitcoin también está determinado por las leyes básicas de oferta y demanda. Cuanto más gente quiera comprarlo, y menos gente quiera venderlo, más sube su precio.



**Transparencia y Previsibilidad:** Gracias al libro de contabilidad público y distribuido, la blockchain, todos pueden verificar todas las transacciones en tiempo real, lo que añade un nivel de transparencia que no se ve en muchos otros sistemas financieros.



*"El valor no es intrínseco, es subjetivo."*

-Carl Menger, Fundador de la Economía Austríaca



## Capítulo #9

Características	¿Por qué bitcoin es buen dinero?
Duradero	Es una moneda digital y no está sujeta al desgaste físico. <i>Como el oro.</i>
Portátil	Se puede almacenar y transferir fácilmente en formato digital; conveniente para llevar a cualquier lugar.
Uniforme	Todo el bitcoin tiene el mismo valor, no importa dónde se use o quién lo posea.
Aceptable	Cada día más personas en todo el mundo aceptan bitcoin como forma de pago.
Escaso	El suministro total de bitcoin es limitado, 21,000,000 para ser exactos, lo que lo hace valioso y deseable.
Divisible	Se puede dividir en unidades más pequeñas, <b>satoshis</b> , lo que permite transacciones más pequeñas.

### Comparando Bitcoin, Oro y Monedas Fiduciarias: La Importancia del Ratio Stock-to-Flow

Piensa en bitcoin, el oro y las monedas fiduciarias como lagos. Cada lago tiene un río que aporta agua, o en este caso, más unidades de valor.



El lago es el "**stock**" (**cantidad total**) y el río es el "**flujo**" (**nuevas unidades añadidas**). La relación entre ambos se llama ratio **Stock-to-Flow (S2F)**.

Si el río añade poca agua al lago, como en Bitcoin y el oro, el ratio S2F es alto, lo que hace que el recurso sea más valioso. Con las monedas fiduciarias como el dólar, los bancos centrales pueden añadir más agua fácilmente, lo que reduce el ratio S2F y posiblemente disminuye su valor por inflación.

En resumen, el alto S2F de Bitcoin lo convierte en una alternativa atractiva a las monedas fiduciarias, ya que su valor está diseñado para mantenerse o aumentar con el tiempo.

	bitcoin	Oro	Moneda fiduciaria
Stock	Alto	Alto	Varía
Flujo	Bajo	Bajo	Alto
Ratio S2F	Alto	Alto	Bajo

# Descubriendo el Valor Real de Bitcoin: Más Allá de la Superficie

## 9.3 Las Múltiples Dimensiones de Bitcoin

Al igual que Internet, que ha evolucionado desde ser un simple canal de comunicación hasta convertirse en una herramienta multifacética, **Bitcoin** también ha mostrado una adaptabilidad y versatilidad notables. No solo funciona como 'dinero digital', sino que también está en constante evolución gracias a mejoras como SegWit, la Red Lightning y Schnorr/Taproot. Estas innovaciones demuestran que la comunidad de **Bitcoin** está activamente trabajando para abordar sus limitaciones y añadir nuevas funcionalidades. Así, incluso si puede parecer 'anticuado' frente a tecnologías más recientes, Bitcoin sigue siendo un proyecto muy activo y relevante en el panorama financiero y tecnológico actual.

### 9.3.1 El Protocolo Base: Bitcoin Core



#### El Cerebro de la Operación

Bitcoin Core actúa como el sistema nervioso central de la red Bitcoin. Heredando las visiones iniciales de Satoshi Nakamoto, esta pieza clave de software es la labor de una comunidad global de desarrolladores que colaboran para mantenerlo y optimizarlo. Al ser de código abierto, cualquiera tiene la oportunidad de estudiar y aportar a su desarrollo, garantizando una mejora continua.

#### Funciones Clave de Bitcoin Core

- **Nodo Completo:** Al operar **Bitcoin** Core, estás validando todo el historial de transacciones de **bitcoin**, actuando como un nodo integral en la red descentralizada.
- **Cartera de Bitcoin:** Este software también incluye una cartera para enviar y recibir bitcoins de forma segura.
- **Minería:** Aunque la minería moderna suele requerir hardware especializado, Bitcoin Core originalmente tenía la capacidad de minar bitcoins.

#### Por Qué **Bitcoin** Core es Especial

Bitcoin Core sigue siendo la versión más fiel a la visión original de Nakamoto y es supervisado por un equipo de desarrolladores apasionados y voluntarios. Este sólido fundamento ofrece una base sobre la cual se pueden construir soluciones innovadoras. Un ejemplo de ello es la **Lightning Network**, que expande las capacidades de **Bitcoin** más allá de lo que se imaginó inicialmente.



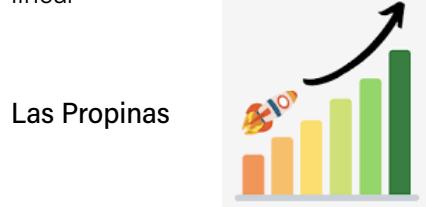
## Capítulo #9

Cuando entendemos que **Bitcoin** no es únicamente una moneda digital, sino también un conjunto de reglas automatizadas, se abren nuevas posibilidades. Un buen ejemplo son las **Inscripciones de Satoshi**, que aprovechan la habilidad de **Bitcoin** para guardar pequeños fragmentos de datos en cada **transacción**. Esto amplía el uso de la **cadena de bloques** de **Bitcoin** para fines diversos, como la salvaguarda de derechos de autor o el almacenamiento de mensajes importantes.



### 9.3.2 Ampliando las Fronteras con la Lightning Network

La red Lightning, que abordamos en el Capítulo 6, facilita **transacciones** rápidas y de bajo costo. Esto hace que **Bitcoin** sea más versátil para aplicaciones del día a día, ya sea para comprar un café o efectuar micropagos en línea.



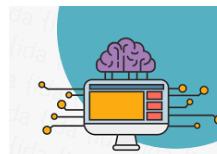
Las "**Zaps**", por ejemplo, son una innovación que está cambiando la forma en que interactuamos en las redes sociales. Similar a los "likes" o los "retweets", las "**Zaps**" son una forma de recompensar a los creadores de contenido, pero en lugar de simplemente ofrecer reconocimiento social, las "**Zaps**" tienen un valor monetario real. Los usuarios pueden ganar **bitcoin** directamente por su contenido, eliminando la necesidad de intermediarios publicitarios y cambiando dramáticamente la economía de las redes sociales. En un futuro en el que **Bitcoin** siga evolucionando, es probable que veamos más innovaciones disruptivas como esta.

### Uso de Stablecoins (Monedas Estables) en la **Red Lightning**

Las stablecoins o monedas estables son criptomonedas diseñadas para mantener un valor estable al estar respaldadas por una reserva de activos, como el dólar estadounidense o el oro. La integración de stablecoins en la **Red Lightning** resalta la versatilidad y adaptabilidad de **Bitcoin**, permitiendo una gama más amplia de usos y ofreciendo más estabilidad en **transacciones** rápidas.

# Descubriendo el Valor Real de Bitcoin: Más Allá de la Superficie

¿Por qué son buenas?



- **Menos Costo:** Enviar dinero a otros países puede ser caro. Con stablecoins en la **Red Lightning** esos costos bajan mucho.
- **Más Acceso:** En lugares donde los bancos no llegan, las stablecoins en la **Red Lightning** ofrecen una nueva forma de pagar y recibir dinero.
- **Rapidez:** Olvídate de esperar días para que llegue una transferencia. Aquí es casi inmediato.
- **Estabilidad:** Estas monedas no saltan de precio como otras criptomonedas, lo que las hace útiles para el día a día.

Pero ten cuidado:

Las stablecoins pueden estar controladas por una sola empresa o grupo. Eso puede ser riesgoso porque pierdes algo de la libertad que da **Bitcoin**. Es algo que debes pensar antes de usarlas.



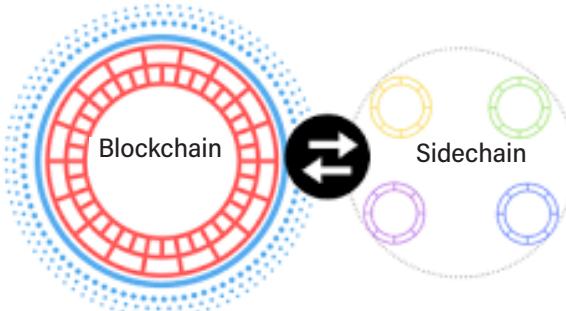
Liquid es una innovación clave que amplía las capacidades de **Bitcoin**, especialmente en términos de **transacciones** rápidas y contratos inteligentes. Funciona como una "cadena lateral", actuando en paralelo a la red principal de **Bitcoin**. Esta configuración permite agilizar las transferencias entre casas de cambio y habilita la creación de tokens, todo sin comprometer la seguridad y descentralización que definen a **Bitcoin**.





## Capítulo #9

Piensa en **Bitcoin** como un juego de ajedrez con un conjunto específico de reglas para mover las piezas. Liquid sería como un tablero adicional situado junto al original. En este tablero alternativo, disfrutas de más flexibilidad para mover tus "piezas" (**bitcoins**) de maneras no permitidas en el tablero principal. Tal vez aquí las piezas se mueven más rápido o de formas completamente nuevas. Lo mejor es que puedes transferir tus piezas de vuelta al tablero original de **Bitcoin** en cualquier momento, manteniendo siempre la seguridad e integridad del sistema.



A diferencia de las soluciones de segunda capa, que operan dentro de la **red de Bitcoin**, las cadenas laterales llevan los **bitcoins** a redes distintas, con reglas y funciones propias. Estos avances hacen de **Bitcoin** una herramienta cada vez más entrelazada en nuestra forma de vivir y manejar el dinero, ajustándose a las múltiples necesidades de cada quién.



### 9.4 Imaginando un Futuro HiperBitcoinizado

Ya estamos viendo cambios transformadores frente a nuestros propios ojos que indican un futuro positivo con **Bitcoin**. Sin embargo, para que **bitcoin** se convierta en la moneda ampliamente aceptada globalmente, aún necesitamos superar obstáculos y lograr avances significativos en áreas como escalabilidad, privacidad, facilidad de uso, descentralización y seguridad. He aquí algunas maneras en las que **Bitcoin** podría moldear nuestro futuro.



**Envíos más baratos:** **Bitcoin** puede reducir significativamente las tarifas de las transferencias internacionales, especialmente de pequeñas cantidades.



**Empoderamiento y Autonomía:** **Bitcoin** puede brindar a las personas control completo sobre su identidad digital y sus bienes, promoviendo la inclusión financiera.



**Cambios en la Política Monetaria:** Con **Bitcoin**, el poder vuelve a estar en manos de la gente, lo que podría llevar a una mayor igualdad económica.

**Innovación FinTech:** **Bitcoin** lidera la innovación en tecnología financiera. Las innovaciones en la capa 2 de **Bitcoin** pueden revolucionar contratos inteligentes, identidad digital y registros de propiedad.

# Descubriendo el Valor Real de Bitcoin: Más Allá de la Superficie



**Educación Financiera:** Bitcoin genera interés en conceptos financieros básicos, lo que podría llevar a una población global más educada financieramente.



**Democratización de las Inversiones:** Bitcoin es accesible a cualquier persona con conexión a internet, lo que podría democratizar las finanzas.



**Evolución de la Banca:** La popularidad de Bitcoin podría forzar a los bancos e instituciones financieras a evolucionar, resultando en mejores servicios y tarifas más bajas.

**Transparencia y Ciberseguridad:** Bitcoin aporta transparencia sin precedentes a las **transacciones** financieras, y su estructura descentralizada minimiza el riesgo de un punto central de ataque.

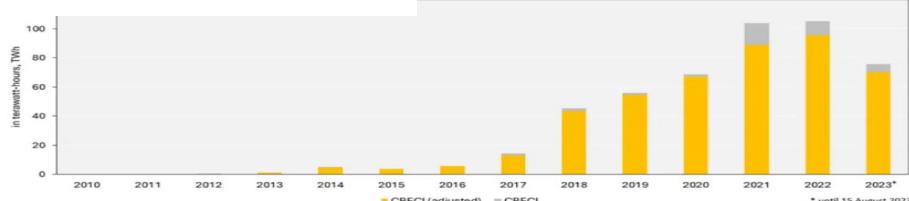
## 9.4.1 Consumo Energético y Sostenibilidad Ambiental en Bitcoin:



Bitcoin permite que los generadores de energía ganen dinero directamente por su producción. Esto podría hacer más estables las redes eléctricas, bajar los precios para los usuarios y aprovechar energía que de otra forma se desperdiciaría. Vamos a expandir un poco sobre este último punto:

La conversación sobre el consumo de energía de Bitcoin ha dado un giro importante. Nuevas estimaciones del Centro de Finanzas Alternativas de la Universidad de Cambridge (CCAF) indican que Bitcoin consume menos energía de lo que se pensaba: 70,4 TWh en lugar de 75,7 TWh. Esto es vital para comprender su verdadero impacto.

### Estimados de el Consumo de Energía por Minería TW/h Bitcoin 2010-2023



### Hardware Más Eficiente

Los avances en hardware de minería, especialmente en equipos ASIC, están detrás de esta revisión. Estos dispositivos son ahora más eficientes en términos energéticos, gracias a la tecnología de semiconductores avanzada. Esta eficiencia contribuye a reducir el consumo general de energía de la red.

### Fuentes de Energía

El nuevo modelo del CCAF también toma en cuenta qué tipos de energía están usando los mineros. Cada vez más, se incorporan fuentes de energía renovable en la operación minera, lo que disminuye el impacto ambiental.

### Perspectiva Global

Para ponerlo en contexto, el consumo energético total de Bitcoin representa apenas el 0,54% del consumo mundial de energía. Es menos que la energía gastada por las secadoras en Estados Unidos.

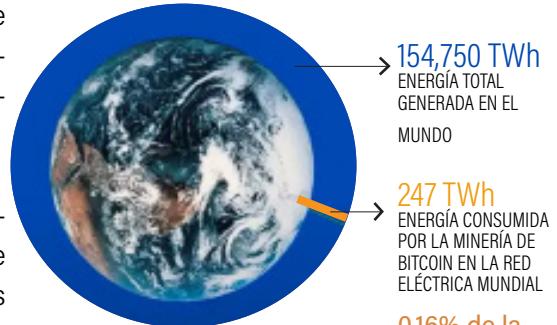


## Capítulo #9

### Rentabilidad en Minería

Por último, JPMorgan ha actualizado su estimación sobre el costo de minar un **bitcoin**, señalando que ahora es de alrededor de \$18,000 dólares, un 14,2% menos que antes. Esta eficiencia aumenta no solo la rentabilidad de la minería sino también la estabilidad y robustez de la red.

La percepción sobre el consumo de energía de **Bitcoin** está cambiando. Con hardware más eficiente y un enfoque en fuentes de energía más limpias, **Bitcoin** está evolucionando para ser más sostenible. Estos datos actualizados son cruciales para el debate sobre su impacto ambiental y su viabilidad a largo plazo.



### 9.4.2 El Efecto Lindy

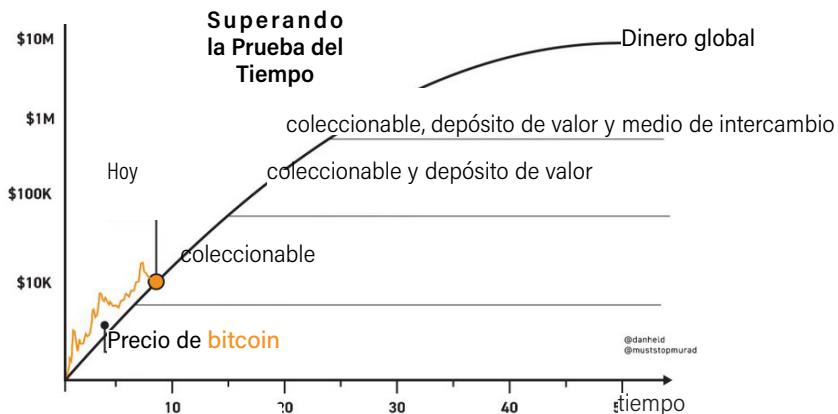
Hemos estado explorando el futuro potencial y el impacto social de **Bitcoin**. Pero no solo su futuro es relevante; también su resistencia y durabilidad hasta la fecha son notables.



Este comportamiento robusto de **Bitcoin** nos lleva a examinar un concepto fascinante conocido como '**Efecto Lindy**'. Según esta idea, si una tecnología ha perdurado durante un tiempo significativo, es más probable que siga existiendo en el futuro. Es como si su longevidad pasada validara su capacidad para seguir siendo relevante.

### El Efecto Lindy

**Bitcoin** no solo muestra signos de un futuro prometedor, sino que su trayectoria hasta ahora lo señala como un claro ejemplo del **Efecto Lindy**. Esto implica que podemos esperar que **Bitcoin** no solo exista en el futuro sino que también siga siendo influyente y valioso.



### Un Futuro Prometedor

Desde su aparición en 2009, **Bitcoin** ha soportado múltiples desafíos, desde ataques informáticos hasta cambios en la regulación. Su habilidad para superar estos obstáculos habla de su carácter descentralizado y resiliencia inherente.

**Bitcoin** está cambiando las reglas del juego. Con mejoras en cómo se usa la energía para la minería y su reconocimiento como moneda en países como El Salvador, **Bitcoin** no solo nos muestra un futuro brillante. Nos está llevando a una nueva forma de entender y usar el dinero que es para todos. Estamos en el comienzo de algo grande, y **Bitcoin** es el protagonista de esta nueva etapa.



# Capítulo #10



## De bits a **Bitcoin**: Ensamblando el Rompecabezas

10.0 Directrices para la Presentación del Proyecto Final  
“Mi Primer **Bitcoin**” y Criterios de Evaluación



# De bits a Bitcoin: Ensamblando el Rompecabezas

*Directrices para la Presentación :*

## *Proyecto Final de "Mi Primer Bitcoin" y Criterios de Evaluación*

*Introducción:*

El proyecto final del curso "*Mi Primer Bitcoin*" es un ensayo de 1 a 2 páginas titulado "*¿Por qué Bitcoin?*", donde se le pedirá que explique qué es **Bitcoin**, cómo funciona y las formas en que cambia el mundo hoy en día.

*Requisitos:*

- El ensayo debe tener un mínimo de 1 página y un máximo de 2 páginas, a doble espacio, con letra de tamaño 12.
- El ensayo debe estar escrito en inglés correcto y sin errores gramaticales ni de ortografía.
- El ensayo debe incluir una introducción, un cuerpo y una conclusión.

*Temas a Cubrir:*

- Explique qué es **Bitcoin** y su historia.
- Explique cómo funciona **Bitcoin**, incluyendo sus características clave como la descentralización, las **transacciones** y la minería.
- Discuta al menos dos formas en que **Bitcoin** cambia la forma en que el mundo opera hoy en día. Proporcione ejemplos y pruebas para respaldar su respuesta.

*Proyecto Alternativo:*

Para aquellos que prefieren una experiencia práctica, pueden participar en la Actividad Final (Simulador de **Bitcoin**) utilizando la herramienta **Bitcoin Blockchain Simulator**: <https://www.bitcoinsimulator.tk/>.

Aquí creará una nueva billetera y recibirá una **clave privada**, lo que le permitirá minar un bloque, **firma transacciones**, crear una **cadena de bloques** privada y realizar un ataque del 51%.



*Criterios de Evaluación:*

Los siguientes criterios se utilizarán para evaluar su proyecto final:

- Claridad en la explicación de lo que es **Bitcoin** y cómo funciona.
- Uso de ejemplos y pruebas para respaldar su respuesta.
- Coherencia y organización del ensayo.
- Uso adecuado de la gramática y la ortografía.
- Relevancia y profundidad de la discusión sobre el tema.



## Capítulo #10

### *Presentación:*

El proyecto final debe presentarse en formato Word o PDF por correo electrónico al instructor del curso antes de la fecha límite especificada en el plan de estudios del curso. No se aceptarán presentaciones tardías.

### *Conclusión:*

El proyecto final es una oportunidad para que muestres tu comprensión de **Bitcoin** y su impacto en el mundo. El ensayo debe demostrar tu capacidad para analizar y sintetizar información y presentarla de manera clara y concisa.

Esperamos que ahora entiendas que **Bitcoin** no es solo una solución técnica a un problema financiero. Es una revolución que reconfigura nuestra relación con el dinero, ofreciendo un futuro más libre, más estable y más inclusivo para todos.

¡Buena suerte con su proyecto final!

*Dalia Platt - Creadora del Currículo y Contenido*

*dplatt@miprimerbitcoin.io*

*@LayerD*

---

¡Felicitaciones, queridos estudiantes! Han desbloqueado el mundo de **Bitcoin**. Han aprendido sobre la tecnología, la historia y los usos de *este dinero* innovador. Pero más allá de todo eso, esperamos que hayan descubierto una nueva forma de pensar sobre el dinero y la libertad financiera.

**Bitcoin** representa una oportunidad única en la historia para tomar el control de nuestras finanzas y protegernos de la inflación y la degradación de las monedas fiduciarias. A través de **Bitcoin**, tenemos la capacidad de tomar decisiones financieras sin depender de los bancos o el gobierno, y eso es algo emocionante y poderoso.

Gracias por asistir al curso. Esperamos que el conocimiento adquirido les emocione y les impulse a seguir aprendiendo.

*El Equipo de Mi Primer Bitcoin*





# Recursos Adicionales



# Recursos Adicionales

## ¿Por qué usar Bitcoin?

- **Película Hard Money** (30 minutos):

Esta película explora la historia del dinero y cómo encaja **Bitcoin** en el sistema financiero actual. Se adentra en los problemas de las monedas fiduciarias tradicionales y cómo **Bitcoin** ofrece una solución.

- **“Por qué Bitcoin” por Wiz:**

Este artículo proporciona una descripción general de los beneficios de usar **Bitcoin** como moneda y reserva de valor. Destaca la naturaleza descentralizada de **Bitcoin** y cómo permite una mayor libertad y seguridad financiera.

- **“El caso alcista de Bitcoin” por Vijay Boyapati:**

Este artículo defiende por qué **Bitcoin** es un activo valioso y por qué tiene el potencial de convertirse en una moneda global dominante. El autor cubre los aspectos técnicos y económicos de **Bitcoin** que lo convierten en una fuerte oportunidad de inversión.

- **“Por qué importa Bitcoin” por Aleks Svetski** (1 hora):

Este video cubre la importancia de **Bitcoin** como un activodigital descentralizado y cómo puede impactar en el sistema financiero actual. El orador explora el potencial de **Bitcoin** para llevar la libertad financiera a las personas de todo el mundo.

<https://fountain.fm/>

## ¿Qué es Bitcoin?

- **“¿Qué es Bitcoin?” por Greg Walker:**

Este artículo proporciona una explicación completa de qué es **Bitcoin**, incluyendo su historia, tecnología y cómo difiere de las monedas tradicionales.

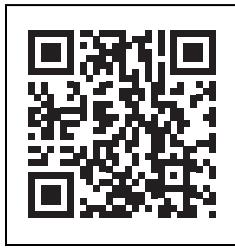
- **“Bitcoin - The Genesis” por RT** (30 minutos):

Este video cubre la creación y los primeros días de **Bitcoin**. Explora las motivaciones del misterioso creador, Satoshi Nakamoto, y cómo evolucionó el concepto de **Bitcoin**.

- **“Comprender Bitcoin” por BJ Dweck** (1 hora 30 minutos):

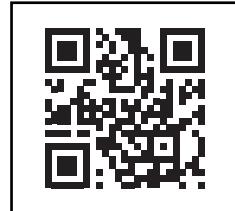
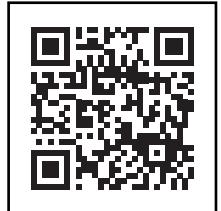
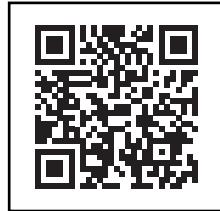
Este video proporciona una explicación detallada de los aspectos técnicos de **Bitcoin** y cómo funciona. El orador cubre temas como la **cadena de bloques**, la minería y la naturaleza descentralizada de **Bitcoin**.

## ¿Cómo ganar y usar Bitcoin?



Elige tu Monedero

Recursos para que los estudiantes aprendan más y se involucren en la comunidad:



Bitcoin Wiki



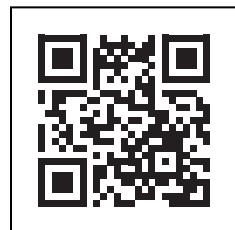
## Aprendizaje Adicional

*The Looking Glass Education*

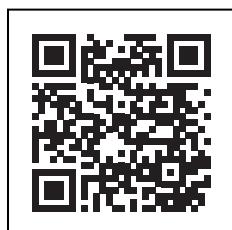


- *El Estándar Bitcoin* (1 hora 40 minutos):

Este audiolibro explora el contexto económico e histórico que llevó a la creación de **Bitcoin**. Cubre los beneficios de una moneda descentralizada y el potencial de **Bitcoin** para convertirse en un estándar global.



Biblioteca Bitcoin



Estudio Bitcoin

- *"Introducción al Pensamiento Austríaco sobre Bitcoin"* (1 hora):

Esta conferencia de audio cubre la Escuela Austríaca de economía y cómo se relaciona con el concepto de **Bitcoin**. Proporciona una mirada profunda a los principios económicos detrás de **Bitcoin** y cómo se alinea con el pensamiento austriaco.

## Autores Importantes

Alex Gladstein	Check Your Financial Privilege
Alex Swan	Terapia de Encuentro Arrraigada: Perspectivas, Características y Aplicaciones
Amanda Cavaleri	<b>Bitcoin</b> y el Sueño Americano: La nueva tecnología monetaria que trasciende nuestra división política
Anita Posch	Aprenda <b>Bitcoin</b> : conviértase en soberano financiero
Daz Bea and Seb Bunney	<b>B</b> is for <b>Bitcoin</b>
Eric Yakes	La 7a Propiedad: <b>Bitcoin</b> y la Revolución Monetaria

# Recursos Adicionales

*Jeff Booth*

El Precio del Mañana: Por Qué la Deflación es la Clave de un Futuro Abundante

*Jimmy Song*

El Pequeño Libro de **Bitcoin**: por qué **Bitcoin** importa para su libertad, finanzas y futuro

*Nik Bhatia*

Dinero por Capas: Del oro y el dólar al **bitcoin** y las monedas digitales de los bancos centrales

*Robert Breedlove*

Gracias a Dios por **Bitcoin**: Creación, corrupción y redención del dinero

---

## Otros Recursos

1. **Bitcoin.org**: Este es el sitio web oficial del proyecto **Bitcoin** y proporciona una gran cantidad de información sobre **Bitcoin**, incluyendo cómo funciona, cómo empezar y cómo usarlo.

2. **Bitcoin Wiki**: Este es un recurso impulsado por la comunidad que proporciona una guía completa de todo lo relacionado con **Bitcoin**. Abarca desde los aspectos técnicos de **Bitcoin** hasta su historia y casos de uso.

3. **Bitcoin Magazine**: Esta es una publicación en línea que cubre noticias y puntos de vista relacionados con **Bitcoin** y otras criptomonedas. Es una buena forma de estar al día de los últimos avances en el ecosistema **Bitcoin**.

4. Coindesk: CCoindesk es un popular sitio de noticias e información que cubre los últimos desarrollos en la industria de las criptodivisas, incluyendo **Bitcoin**.

5. **Bitcointalk**: **Bitcointalk** es un foro donde los usuarios pueden discutir temas relacionados con **Bitcoin**, hacer preguntas y compartir información. Es un lugar ideal para aprender de otros entusiastas y expertos en **Bitcoin**.

6. **Blockchain.info**: Se trata de un popular explorador de **blockchain** que permite a los usuarios ver y explorar la **blockchain** de **Bitcoin** en tiempo real. Proporciona gran cantidad de información sobre **transacciones** individuales, bloques y **direcciones**.

7. **Bitcoin Core**: Este es el software original de **Bitcoin** y sigue siendo ampliamente utilizado por muchos usuarios y desarrolladores. Proporciona un potente conjunto de herramientas para interactuar con la red **Bitcoin** y construir aplicaciones **Bitcoin**.

8. **Electrum**: Electrum es un popular monedero **Bitcoin** que proporciona una forma sencilla y segura de almacenar y gestionar **Bitcoin**. También es altamente personalizable y proporciona una amplia gama de características para usuarios avanzados.



Los Monederos HD hacen todo más fácil y seguro en **Bitcoin**. Antes, cada **transacción** necesitaba una nueva clave, y tenías que hacer un respaldo siempre. Ahora, con los Monederos HD, usas una "semilla" de 12-24 palabras para crear muchas claves. Esta semilla crea un árbol de **claves privadas** y públicas.

La **clave pública** extendida, o xPub, permite hacer **direcciones** públicas nuevas. Pero no da acceso a tus fondos. Aun así, no la compartas, porque alguien podría ver todas tus **transacciones**.

¿Por qué son buenos los Monederos HD? Primero, con la semilla puedes recuperar todo, así que es más fácil hacer respaldos. Segundo, son más privados porque usas una clave nueva cada vez. Tercero, son seguros porque la **clave privada** nunca está en línea. Y por último, son prácticos porque no necesitas hacer un respaldo cada vez que haces una **transacción**.

---

En **Bitcoin**, hay diferentes tipos de **direcciones** para recibir y enviar dinero, un poco como diferentes tipos de cuentas bancarias pero para **Bitcoin**. Los tipos más comunes son las **direcciones** que empiezan con "1", las que empiezan con "3" y las que empiezan con "bc1". Cada tipo tiene sus propias ventajas, como mayor seguridad o menores tarifas.

Para el usuario final, lo más importante es saber que no todos los monederos o servicios aceptan todos los tipos de **direcciones**. Así que a veces, tendrás que convertir de un tipo a otro para hacer una **transacción**. Pero en general, mientras más nuevo sea el tipo de **dirección**, más segura y barata será la **transacción**.

Tipo de dirección BTC	Características Principales	Ventajas	Desventajas
Legacy (P2PKH)	Empiezan con "1"	Totalmente compatible con todos los servicios	- <b>transacciones</b> más grandes -tarifas más altas
Nested SegWit (P2SH)	Empiezan con "3"	Más eficiente que Legacy	Menos eficiente que Native SegWit pero más compatible
Native SegWit (bech32)	Empiezan con "bc1q"	Menores tarifas <b>transacciones</b> más pequeñas	No completamente compatible con todos los servicios
Taproot (P2TR)	Empiezan con "bc1p"	Mayor privacidad <b>transacciones</b> complejas eficientes	Nueva y con compatibilidad limitada por ahora



## Prevenir Estafas en Bitcoin: Protege tus bitcoin

En la frontera digital de **Bitcoin**, la promesa de ganancias rápidas puede atraer a inversores desprevenidos a estafas sofisticadas. Esta sección se dedica a educar a los usuarios sobre cómo detectar y prevenir estafas en **Bitcoin**, salvaguardando su inversión y manteniendo segura su experiencia en el mundo de **Bitcoin**.

**Las estafas encubiertas y firma ciega:** Las estafas más comunes y las usuarios deben estar siempre alerta. Nunca deben revelar sus **claves privadas** y siempre deben entender completamente las **transacciones** antes de confirmarlas.

**1. Estafas de phishing:** El estafador se hace pasar por un servicio legítimo de **Bitcoin** y envía un correo electrónico a la víctima pidiéndole que inicie sesión en su cuenta. El correo electrónico contiene un enlace a un sitio web falso que se parece al servicio legítimo, y cuando la víctima introduce sus credenciales de inicio de sesión, el estafador las captura y luego puede acceder a la cuenta de la víctima.

**Ejemplo:** "Hola, somos de [Exchange de **Bitcoin**] y hemos detectado actividad sospechosa en su cuenta. Por favor, haga clic en este enlace para verificar su cuenta".

**2. Estafas de inversión:** Las estafas de inversión prometen rendimientos garantizados o "demasiado buenos para ser ciertos" a cambio de un depósito de **Bitcoin**. A menudo operan en un esquema Ponzi, utilizando los fondos de los nuevos inversores para pagar a los antiguos hasta que el esquema se derrumba.

**Ejemplo:** "¡Invierta con nosotros y obtenga un retorno del 10% diario! ¡Garantizado! Solo necesita depositar una pequeña cantidad de **bitcoin** para comenzar"

**3. Estafas de la doble cantidad de bitcoin:** Un estafador promete enviar el doble de la cantidad de **Bitcoin** que le envías. Esta estafa se popularizó por un hackeo de Twitter en 2020, donde cuentas de alto perfil prometían duplicar cualquier cantidad de **Bitcoin** enviada.

**Ejemplo:** "Envíe 0.1 **BTC** a esta **dirección**, y le devolveremos 0.2 **BTC** inmediatamente!"

**4. Estafas de soporte técnico falso:** El estafador se hace pasar por soporte técnico de un servicio de **Bitcoin** y solicita acceso a la computadora o cuenta de la víctima para "resolver un problema".

**Ejemplo:** "Hola, soy de [Servicio de billetera **Bitcoin**], parece que hay un problema con su cuenta. Proporcioneme sus datos de inicio de sesión para solucionarlo".

**5. Estafas de esquemas piramidales:** En estas estafas, los inversores iniciales reciben grandes pagos en **Bitcoin** con dinero invertido por personas que se unen más tarde al esquema. A medida que más personas se unen, los inversores iniciales y los organizadores se benefician mientras los últimos en unirse sufren pérdidas cuando la pirámide colapsa.

**Ejemplo:** "Únete a nuestro programa de inversión y recibe rendimientos masivos. Cuantas más personas invites, más ganarás."



**6. Estafas de monedas falsas:** Los estafadores crean una nueva "criptomoneda" y piden a las personas que inviertan en su ICO (Oferta Inicial de Monedas). Una vez que se recauda suficiente dinero, los estafadores desaparecen.

**Ejemplo:** "Somos XYZ Coin, la próxima gran criptomoneda. Invierte en nuestra ICO para recibir beneficios masivos."

**7. Estafas de minería en la nube:** Los estafadores venden contratos de minería en la nube que prometen rendimientos elevados. A menudo, estos contratos son falsos y los estafadores simplemente se quedan con los bitcoins que las personas utilizan para comprar los contratos.

**Ejemplo:** "Compre nuestro contrato de minería en la nube y gane bitcoins pasivamente. Sin hardware necesario, sin complicaciones."

**8. Estafas de bots de comercio:** Los estafadores venden software o bots que prometen altos rendimientos a través del comercio automatizado de Bitcoin. En realidad, estos bots pueden ser ineficaces o incluso robar directamente Bitcoin de las carteras de los usuarios.

**Ejemplo:** "Nuestro bot de comercio de criptomonedas utiliza IA avanzada para garantizar un 80% de operaciones ganadoras. Pruébalo ahora y observa cómo crecen tus bitcoins"

**9. Estafas de regalos:** Similar a la estafa de la doble cantidad de Bitcoin, pero en este caso, los estafadores piden a los usuarios que envíen Bitcoin o datos personales para calificar para un regalo gratuito.

**Ejemplo:** "Como agradecimiento a nuestra comunidad, estamos regalando 500 BTC. Simplemente envíe 0.01 BTC a esta dirección para calificar."

**10. Estafas de "soporte técnico":** Los estafadores se hacen pasar por personal de soporte técnico de una empresa de tecnología o criptomonedas. Pueden convencer a los usuarios de que hay un problema con su billetera de Bitcoin y solicitar el acceso para "resolver" el problema, pero luego roban los fondos.

**Ejemplo:** "Somos del soporte técnico de XYZ Wallet. Hemos detectado un problema con tu billetera. Por favor, proporciona tus detalles de inicio de sesión para que podamos solucionarlo."

**11. Estafas de trabajos falsos :** Los estafadores pueden publicar ofertas de trabajo falsas, pidiendo a los solicitantes que paguen una tarifa de procesamiento en Bitcoin. También pueden ofrecer pagos elevados por trabajos de "procesamiento de Bitcoin", donde el empleado se convierte en un intermediario para transacciones de dinero posiblemente ilegales.

**Ejemplo:** "Estamos contratando procesadores de Bitcoin. El salario es de 1 BTC por semana. Solo necesitas procesar transacciones desde tu propia billetera."

**12. Estafas de ransomware:** El estafador cifra los datos del usuario y exige un pago en Bitcoin para desbloquearlo. Este tipo de estafa es común en ataques de ransomware.

**Ejemplo:** "Hemos cifrado sus datos. Pague 0.5 BTC a esta dirección para obtener la clave de descifrado".



# Glosario

# Glosario

**Activodigital:** una representación digital de valor que se puede negociar o utilizar como reserva de valor, como **Bitcoin**.

**Almacenamiento en frío:** un método de almacenamiento de **bitcoins** fuera de línea, lejos del riesgo de hackers u otras amenazas en línea.

**Altcoins:** otras monedas digitales similares a **Bitcoin**.

**Banca de reserva fraccional:** un sistema bancario en el que los bancos mantienen solo una fracción de los depósitos en efectivo como reservas.

**Banca restrictiva:** Restricciones o limitaciones en los servicios bancarios o el acceso a los servicios bancarios.

**Banco central (Fed):** una institución propiedad del gobierno que gestiona la política monetaria de un país.

**Billetera caliente:** una billetera **Bitcoin** que está conectada a Internet, lo que permite un fácil acceso a los **bitcoins**.

**Billetera:** Un contenedor virtual para **bitcoin** similar a una billetera física, que contiene clave(s) privada(s) que le permiten gastar el **bitcoin** asignado a ella en la **cadena de bloques**.

**Bitcoin:** la tecnología, la comunidad, el protocolo y el software.

**bitcoin:** una moneda digital que permite a las personas enviarse dinero sin usar un banco.

**Blockchain:** un registro público de todas las **transacciones** de **Bitcoin** que han tenido lugar.

**BTC:** la unidad utilizada para **Bitcoin**. Una moneda digital que se puede usar para hacer compras o negociarse.

**Canasta de bienes:** colección de bienes o servicios utilizados para medir los cambios en el costo de vida.

**Centralización:** la concentración de poder o control en una sola entidad.

**Clave privada:** Un dato secreto que prueba el derecho de una persona a gastar **bitcoin** desde una billetera específica a través de una **firma** criptográfica.

**Clave pública/Dirección de Bitcoin:** una contraseña/número público utilizado para recibir **bitcoins**.

**Confirmación:** proceso por el cual una **transacción** es procesada por la red y es muy poco probable que se revierta. El método "mineros" verifican la autenticidad de las **transacciones** con su hardware y software de computadora. Se recomienda esperar al menos 6 confirmaciones para evitar el doble gasto.



**Contrato inteligente:** Un contrato autoejecutable con los términos del acuerdo escritos en código.

**Control de capitales:** restricciones al movimiento de dinero a través de las fronteras.

**Copia de seguridad de la billetera:** Una copia de las **claves privadas** y la frase de recuperación/palabra clave de semilla de una billetera de **Bitcoin**, que se puede usar para restaurar el acceso a la billetera en caso de pérdida o robo del original.

**Criptografía:** una rama de las matemáticas que ayuda a crear sistemas seguros

**Debasement:** la reducción del valor de una moneda, a menudo reduciendo la cantidad de metal precioso en una moneda.

**Descentralización:** la distribución de poder y control en una red, en lugar de tener una autoridad central.

**Deuda:** dinero que se debe a otra persona.

**Devaluación:** una disminución del valor de una moneda en relación con otras monedas.

**Dinero de mercancía:** objetos que tienen valor en sí mismos y se utilizan como medio de cambio, como el oro o la plata.

**Doble coincidencia de deseos:** el fenómeno en el que dos partes en una economía de trueque tienen lo que quiere la otra parte y quieren lo que tiene la otra parte.

**Doble gasto:** cuando una persona intenta gastar su **bitcoin** en dos destinatarios diferentes al mismo tiempo.

**Exportaciones:** bienes y servicios producidos en un país y vendidos a otro país.

**Fiat:** dinero que no está respaldado por una mercancía, sino que recibe valor por decreto gubernamental.

**Firma:** Un mecanismo matemático que permite a alguien probar la propiedad.

**Fork duro:** un cambio en el protocolo de **Bitcoin** que crea una nueva versión de la **cadena de bloques**, que no es compatible con la versión anterior.

**Frase de recuperación/palabra clave de semilla:** una serie de 12, 18 o 24 palabras que se pueden usar para generar múltiples pares de **claves privadas** y públicas. Estos se pueden usar para restaurar una billetera de **Bitcoin**.

## Glosario

**ID de transacción**: una cadena de números y letras que muestra los detalles de una transferencia de **Bitcoin** (como la cantidad enviada, las **direcciones** del remitente y el destinatario y la fecha de la transferencia) en la **cadena de bloques** de **Bitcoin**.

**Importaciones**: bienes y servicios producidos en otro país y vendidos en el mercado nacional.

**Inflación**: un aumento en el nivel general de precios de bienes y servicios en una economía.

**Libro blanco**: un informe que explica el problema y la solución que un proyecto de **cadena de bloques** o criptomoneda intenta abordar.

**Libro de contabilidad**: un registro de **transacciones** financieras.

**Libro mayor distribuido**: una base de datos que se extiende por una red de computadoras, en lugar de estar almacenada en una ubicación central.

**Medios de intercambio**: objetos o sistemas ampliamente aceptados en el intercambio de bienes y servicios.

**Minería**: El proceso de utilizar hardware de computadora para hacer cálculos matemáticos para la **red de Bitcoin** para confirmar **transacciones** y aumentar la seguridad.

**Nodo Ligero**: Un cliente de **Bitcoin** que solo almacena una cantidad limitada de datos de la **cadena de bloques**, en lugar de la cadena completa.

**Nodo**: Una computadora o dispositivo que está conectado a la **red de Bitcoin** y participa en la verificación y transmisión de **transacciones**.

**Oferta inicial de monedas (ICO)**: un método de recaudación de fondos en el que se vende una nueva criptomoneda a inversores a cambio de una criptomoneda más establecida, como **Bitcoin**.

**Oferta monetaria**: La cantidad total de dinero en circulación en una economía.

**P2P**: Sistemas peer-to-peer que funcionan como un colectivo, permitiendo que cada individuo interactúe directamente con otros.

**Peg**: Una tasa de cambio fija entre dos monedas, donde una está vinculada al valor de otra.



**PIB:** producto interno bruto, el valor total de bienes y servicios producidos en un país en un período de tiempo determinado.

**Poder adquisitivo:** La capacidad del dinero para comprar bienes y servicios.

**Política monetaria y fiscal:** Las políticas de un banco central y del gobierno, respectivamente, que influyen en la oferta monetaria y las tasas de interés en una economía.

**Prueba de trabajo:** Un mecanismo de consenso que requiere que los usuarios realicen una cierta cantidad de trabajo computacional para participar en la red.

**Ratio de reserva:** La proporción de depósitos que un banco debe mantener como reservas.

**Red:** Un grupo de entidades interconectadas.

**Satoshi:** la unidad más pequeña de **Bitcoin**, equivalente a 1/100,000,000 de un **bitcoin**. Está nombrado en honor al creador de **Bitcoin**, Satoshi Nakamoto.

**SegWit (Segregated Witness):** Una actualización del protocolo **Bitcoin** que cambia la forma en que se almacenan los datos en la **cadena de bloques**, permitiendo una mayor capacidad y tarifas de **transacción** más bajas.

**Sin bancarizar:** Individuos o comunidades sin acceso a servicios bancarios tradicionales.

**Sistema centralizado:** un sistema en el que el poder o el control se concentra en una sola entidad.

**Sistema descentralizado:** un sistema en el que el poder o el control se distribuye entre múltiples entidades.

**Subasta:** proceso por el cual los bienes o activos se venden al postor más alto.

**Tasa de hash:** una forma de medir la potencia de procesamiento de la red **Bitcoin**.

**Tipo de cambio:** el valor de una moneda en relación con otra.

**Trueque:** intercambio de bienes y servicios sin el uso de dinero.

**Unidad de cuenta:** Una unidad de medida estándar utilizada para expresar el valor de bienes y servicios.

**Valor temporal del dinero:** El principio de que el dinero vale más en el presente que en el futuro.

**XBT y BTC:** abreviaturas de **bitcoin**.





## Información Adicional

**Influencia del precio:** Tanto la minería de oro como la minería de **bitcoin** están sujetas al precio del metal precioso o del **bitcoin** en el mercado. Sin embargo, aquí es donde se destaca una diferencia significativa. Mientras que el precio del oro y otros metales preciosos puede estar influenciado por una variedad de factores económicos y políticos, el precio del **bitcoin** es influenciado de manera más directa por la oferta y demanda en su propio mercado sin intervención de gobiernos o bancos centrales.

Esta característica única del **bitcoin** como una moneda descentralizada le permite tener una mayor independencia de los factores externos y, potencialmente, contribuir a una mayor estabilidad del mercado en comparación con la minería tradicional que depende de la economía global y otros factores externos.





## Ejercicio de organizar una Transacción de Principio a Fin

1. Una usuaria (llamémosla Mina) desea enviar bitcoins a otro usuario (Jaime). Mina crea una transacción que incluye la dirección de Bitcoin de Jaime (el destinatario), la cantidad de bitcoins que se enviarán y una referencia a los bitcoins que posee y que serán enviados (esto se refiere a las salidas de transacciones pasadas que son propiedad de Mina).
2. Mina luego utiliza su clave privada para firmar la transacción. Esta firma digital es una prueba de que la transacción proviene de Mina y no ha sido alterada durante su transmisión.
3. La transacción firmada se transmite a la red Bitcoin, donde es recogida por los nodos de la red. Estos nodos validan la transacción comprobando la firma digital con la clave pública de Mina, que está asociada con su dirección de Bitcoin y se puede encontrar en la cadena de bloques.
4. Los nodos también comprueban que las entradas de la transacción (las salidas de las transacciones anteriores que Mina está gastando) no se hayan gastado antes y que Mina tiene suficientes bitcoins para enviar la cantidad especificada a Jaime.
5. Una vez que la transacción ha sido validada, se coloca en el mempool, una especie de "sala de espera" para las transacciones que están esperando ser incluidas en un bloque por los mineros.
6. Los mineros recogen las transacciones del mempool y las agrupan en un bloque candidato. Para decidir qué transacciones incluir, suelen dar preferencia a las transacciones que ofrecen las tasas de transacción más altas.
7. Los mineros utilizan un algoritmo de hash para intentar resolver un problema matemático que implica su bloque candidato y el hash del bloque anterior en la cadena de bloques. Este proceso es conocido como "prueba de trabajo" y requiere un considerable poder de cálculo.
8. Cuando un minero resuelve el problema, transmite el bloque a la red. Los otros nodos de la red comprueban el trabajo realizado y, si es correcto, añaden el bloque a su versión de la cadena de bloques.
9. Una vez que el bloque ha sido añadido a la cadena de bloques, la transacción de Mina a Jaime se considera confirmada. Jaime puede entonces gastar los bitcoins que recibió utilizando su clave privada para firmar una nueva transacción.
10. El bloque que incluye la transacción de Mina se convierte en parte del registro inmutable y transparente de todas las transacciones en la cadena de bloques. Y el proceso de minería comienza de nuevo con los mineros intentando resolver el problema de la prueba de trabajo para el siguiente bloque.

# Información Adicional

Reyna comienza creando la **transacción**. Esta **transacción** representa la intención de Reyna de enviar un **bitcoin** a Luis.

1. Reyna abre su billetera y escanea la **dirección** de **Bitcoin** de Luis. Esta **dirección** es una cadena de caracteres que es única para Luis, algo así como su cuenta de correo electrónico, pero para **Bitcoin**. Puede parecerse a algo así: 3FZbgi29cpjq2GjdwV8eyHuJNkLktZc5. Reyna puede escanear esta **dirección** en forma de código QR o puede copiarla y pegarla en su monedero digital.

2. A continuación, Reyna debe ingresar la cantidad de **bitcoins** que desea enviar a Luis. Aquí es donde “**llena el importe**”. Además decide cuánto está dispuesta a pagar como tarifa de **transacción** para que los mineros confirmen y registren la **transacción** en la **blockchain** de **Bitcoin**. Esta es la parte de “**llenar la tarifa**”.

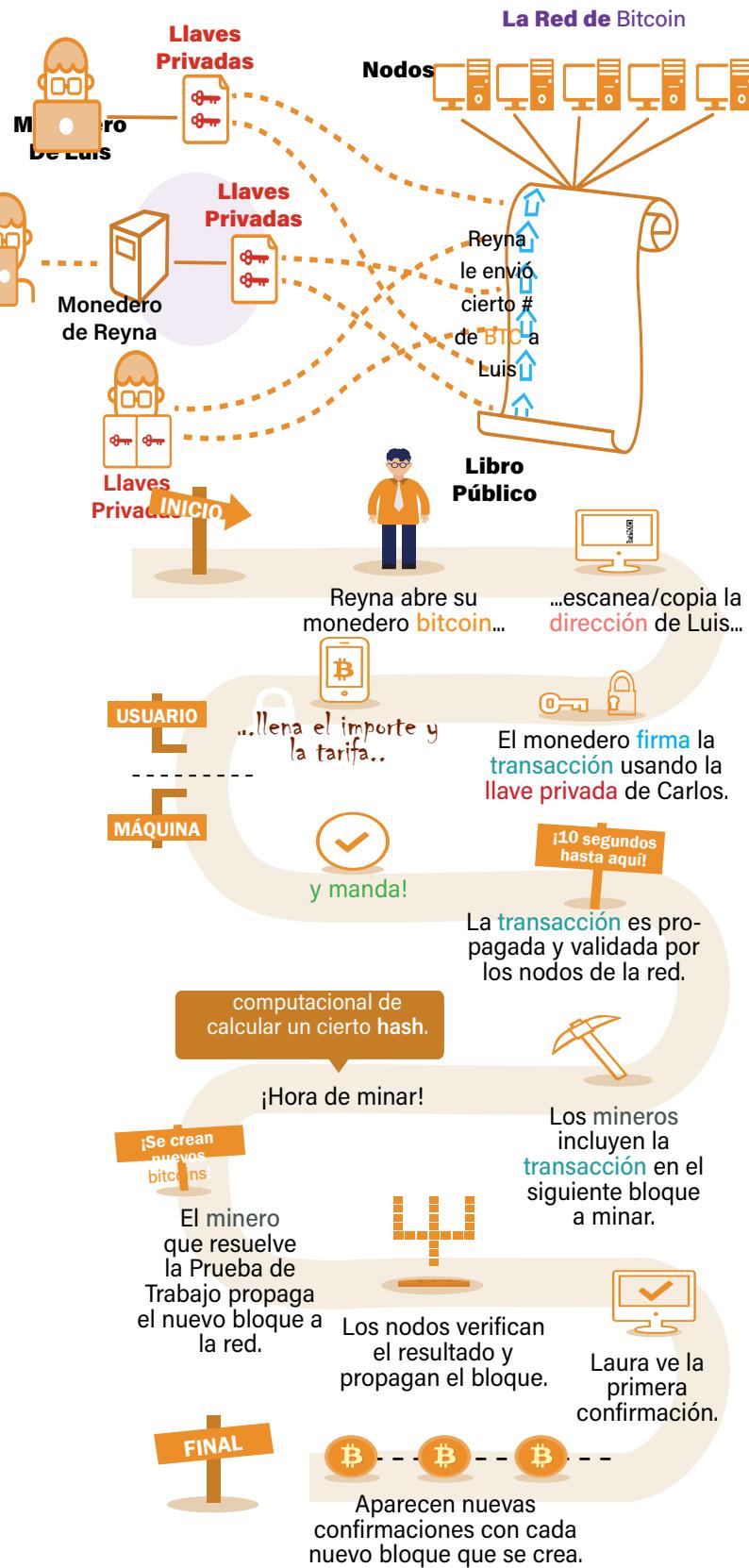
3. Una vez que ha decidido el importe y la tarifa, Reyna utiliza su **clave privada** para firmar digitalmente la **transacción**. Esta es la primera etapa en la que se utiliza la criptografía.

4. La **transacción**, que ahora incluye la **firma digital** de Reyna, se transmite a la red **Bitcoin**.

5. Los mineros en la **red de Bitcoin** luego intentan confirmar la **transacción**. Lo hacen verificando la **firma digital** de Reyna utilizando la **clave pública** asociada que está disponible en la **blockchain**. Esta es la segunda etapa en la que se utiliza la criptografía.

6. Una vez que los mineros confirman que la **firma digital** es válida (es decir, que la **transacción** realmente proviene de Reyna), registran la **transacción** en un nuevo bloque en la **cadena de bloques** de **Bitcoin**.

7. La **dirección** de **Bitcoin** a la que Reyna está enviando los **bitcoins** está vinculada a la **clave pública** de Luis. Esta **clave pública** de Luis se utiliza en la **transacción** principalmente para identificar su **dirección** de **Bitcoin**.





## Un Vistazo Técnico a las Transacciones de Bitcoin

El script de bloqueo contiene la **dirección** del destinatario y verifica que se haya utilizado la **clave privada** correcta. Esto garantiza que las **claves privadas** permanezcan confidenciales y estén protegidas de forma segura.

Para desbloquear los fondos, el remitente debe demostrar la propiedad generando una **firma digital** con su **clave privada**, confirmando así la posesión de la **dirección**. Por ejemplo, digamos que quieras enviar algunos **bitcoins** a un amigo, pero quieras asegurarte de que tu amigo solo pueda gastarlos después de una fecha determinada. Puedes usar el script de **Bitcoin** para definir esta condición, conocida como "bloqueo de tiempo". Al crear la **transacción**, incluyes un script que especifica la condición de bloqueo de tiempo. Cuando tu amigo recibe los **bitcoins**, solo puede gastarlos después de que haya pasado la fecha especificada.

El script de **Bitcoin** también se puede utilizar para crear condiciones más complejas para gastar **bitcoins**, como **transacciones** de múltiples firmas, que requieren que varias partes autentiquen una **transacción** antes de que pueda ser gastada. Esto puede ser útil en situaciones en las que varias partes necesitan aprobar una **transacción**.

En términos sencillos, el script ayuda a garantizar la seguridad y confiabilidad de las **transacciones** de **Bitcoin** utilizando **claves privadas** y públicas para verificar la propiedad y transferencia de fondos. Los diferentes métodos de **transacciones** tienen diferentes niveles de seguridad. Algunos revelan la **clave pública** del destinatario durante la **transacción**, lo que puede añadir un nivel adicional de seguridad o permitir condiciones más complejas para gastar los **bitcoins**, como en el caso de las **transacciones** con múltiples firmas.



Aunque hemos cubierto muchos aspectos fundamentales, aún queda mucho por aprender sobre **Bitcoin** y su scripting. Para aquellos que deseen profundizar un poco más, recomendamos visitar [learnmeabitcoin.com](http://learnmeabitcoin.com) y explorar la información disponible allí. Además, puedes escanear el código QR adjunto para obtener más recursos y aprendizajes. ¡Feliz aprendizaje!

## Información Adicional

### Monederos HD

Antiguamente, con cada **transacción** de la **cadena de bloques**, se generaba una nueva **clave privada** y pública, no relacionadas con las claves anteriores. Esto significaba que los usuarios tenían que respaldar su clave y la información de su cartera después de cada **transacción**. Con el crecimiento de la **cadena de bloques**, este sistema de "Just a Bunch of Keys" fue mejorando.

El verdadero avance llegó con la Propuesta de Mejora de **Bitcoin** (BIP32), que introdujo los Monederos Deterministas Jerárquicos (HD) y las claves extendidas. Un Monedero HD es un monedero centrado en la privacidad para la generación de **direcciones**, la gestión de claves y la recuperación.

Lo que distingue a estos monederos es el tipo de gestión de pares de claves que permite generar nuevas **direcciones** a partir de una semilla raíz, que es esencialmente una larga **cadena de datos**. Esta cadena se formatea en 12-24 palabras (frase de semilla o frase mnemotécnica) para facilitar su uso. La semilla genera automáticamente una estructura de árbol de **claves privadas** y públicas derivadas de un par de claves maestras, conocido como **clave privada** extendida (xPriv) y **clave pública** extendida (xPub).

La clave xPub te permite衍生 nuevas **direcciones** públicas sin necesidad de acceder a ninguna **clave privada**. No contiene ninguna información sobre las **claves privadas** y no te da acceso a los fondos ni capacidad de gasto. Sin embargo, es muy arriesgado compartir el xPub con alguien, ya que con él, una persona puede ver tu historial de **transacciones** completo y todas las **direcciones** públicas y saldos asociados.

Los Monederos HD son beneficiosos por varias razones. Permiten un fácil respaldo y recuperación, ya que el sistema determinista y jerárquico significa que el monedero puede regenerarse y recuperarse por completo con el uso de una sola frase semilla. Mejoran la privacidad, ya que un usuario puede generar diferentes claves para cada **transacción**, ocultando así el historial de **transacciones** y el saldo total exacto al público. También son seguros, ya que la **clave privada** siempre se almacena offline, eliminando el riesgo de ataques cibernéticos. Por último, son convenientes y eficientes, ya que no es necesario respaldar cada **dirección** después de cada **transacción**.



## Tras los Bloques: El Misterio de la Programación en Bitcoin

Script es un lenguaje de programación utilizado en **Bitcoin** para crear contratos inteligentes y automatizar **transacciones**. Para entender Script, es útil pensar en él como un conjunto de instrucciones que le indican a la Red de **Bitcoin** qué hacer con una **transacción** específica.

Piensa en ello como una máquina expendedora. Insertas dinero, haces una selección, y la máquina dispensa automáticamente tu artículo. De la misma manera, un **contrato inteligente** ejecuta automáticamente los términos del acuerdo entre dos partes, sin la necesidad de intermediarios como abogados o bancos.



Por ejemplo, un contrato inteligente podría utilizarse para representar un acuerdo financiero, como un préstamo o un bono. Los términos del acuerdo, como la tasa de interés y el calendario de pagos, se codifican en el contrato. Cuando se cumplen las condiciones acordadas, el contrato ejecuta automáticamente los términos y transfiere los fondos. Los contratos inteligentes son transparentes, seguros y autoejecutables, lo que puede ayudar a reducir los costos y riesgos asociados con los procesos contractuales tradicionales. Además, dado que existen en una red descentralizada, son resistentes a la manipulación o interferencia, lo que los convierte en una forma más segura y confiable de realizar **transacciones**.

De manera similar, **Bitcoin** utiliza **Script** para asegurarse de que se cumplan condiciones específicas antes de procesar una **transacción**.

Aunque otras redes de **blockchain**, como Ethereum, también soportan contratos inteligentes y **transacciones** programables, utilizan diferentes lenguajes de programación y enfoques para hacer cumplir las reglas y condiciones de las **transacciones**. Solo **Bitcoin** usa **Script**.

Script es un lenguaje de programación muy básico, pero lo suficientemente potente como para manejar una amplia gama de **transacciones**. Por ejemplo, puede utilizarse para crear **transacciones** de firmas múltiples, donde varias personas deben autorizar una **transacción** antes de que pueda ser procesada, o para crear un contrato inteligente, donde una **transacción** se ejecuta automáticamente cuando se cumplen ciertas condiciones.

El concepto detrás de **Script** puede parecer complejo, pero en realidad es bastante simple. Al utilizar **Script**, la Red de **Bitcoin** puede hacer cumplir automáticamente las reglas y condiciones de las **transacciones**, lo que lo convierte en una forma segura y eficiente de transferir valor.



Un contrato inteligente es un programa informático que se ejecuta automáticamente cuando se cumplen ciertas condiciones preestablecidas en una red **blockchain**.

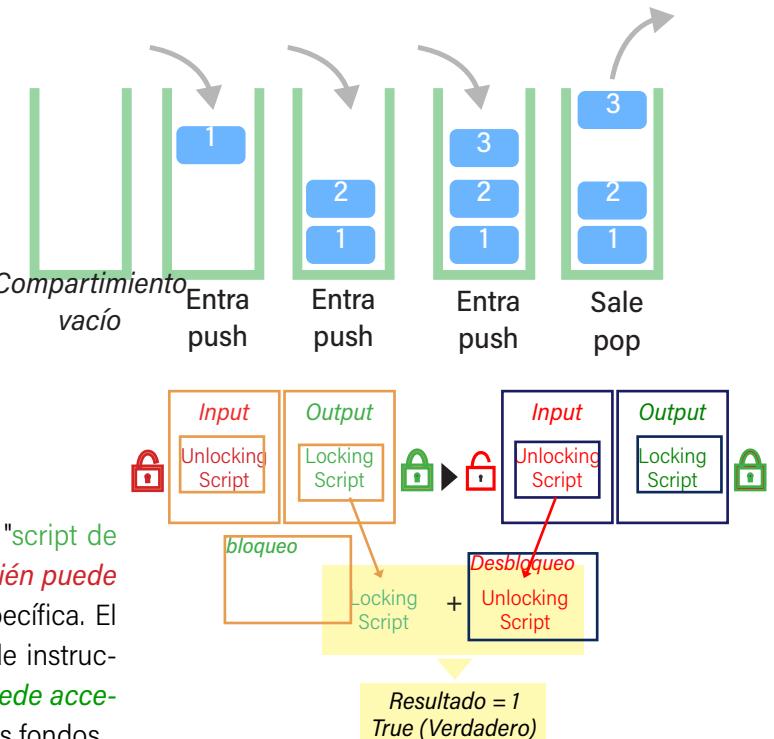
# Información Adicional

## Cómo se Aplica la Programación en las [Transacciones](#) de Bitcoin

Imagina una pila de platos en la que puedes añadir un nuevo plato en la cima de la pila (esta operación se llama “[push](#)”) y también puedes quitar el plato de la cima de la pila (esta operación se llama “[pop](#)”). El último plato que colocas en la pila será el primero que puedes sacar.

En [Bitcoin](#), los scripts funcionan de una manera similar a esta pila de platos. Se utiliza una estructura de datos llamada “pila” que sigue la regla LIFO (Last In, First Out), que significa “último en entrar, primero en salir”. Así que, al igual que el último plato que pusiste en la pila es el primero que puedes quitar, el último dato que se añade a la pila en un script de [Bitcoin](#) es el primero en ser procesado.

Una [transacción](#) básica de [Bitcoin](#) utiliza al menos un “script de bloqueo” y un “script de desbloqueo” para determinar [quién puede acceder a los fondos](#) en una [dirección](#) de billetera específica. El [script de bloqueo](#) puede considerarse como una lista de instrucciones que describen [cómo el receptor de los fondos puede acceder a ellos](#), mientras que el script de desbloqueo libera los fondos.



Supongamos que tenemos un script de [Bitcoin](#) muy básico que utiliza los operadores [OP-ADD](#) y [OP-EQUAL](#).

Este script puede verse algo así:

`2 2 OP-ADD 4 OP-EQUAL`

Este script suma dos números (2 y 2) utilizando [OP-ADD](#), y luego compara el resultado con 4 utilizando [OP-EQUAL](#).

La ejecución de este script procede así:

Los dos primeros números (2 y 2) son empujados a la pila.

Pila: [2, 2]

El operador [OP-ADD](#) toma los dos primeros elementos de la pila (los dos 2s), los saca de la pila, los suma, y pone el resultado (4) de vuelta en la pila.

Pila: [4]

4 es empujado a la pila.

Pila: [4, 4]

Finalmente, [OP-EQUAL](#) toma los dos primeros elementos de la pila (los dos 4s), los saca de la pila, comprueba si son iguales, y pone el resultado (True) de vuelta en la pila.

Pila: [True]

Como puedes ver, el último elemento que se añade a la pila (en este caso, los números que se suman y el número con el que se compara el resultado) es el primero que se quita cuando se ejecutan los operadores [OP-ADD](#) y [OP-EQUAL](#). Así es como los scripts de [Bitcoin](#) utilizan una estructura de pila que sigue la regla LIFO.



## Trading e Inversión en bitcoin

Exploraremos el tema del comercio y la inversión en **Bitcoin**, pero es importante señalar que el objetivo principal del uso de **Bitcoin** no es obtener beneficios a corto plazo a través del comercio especulativo. En su lugar, el objetivo principal es protegerse de la inflación y de la potencial destrucción de los sistemas tradicionales de moneda fiduciaria. Aunque es posible utilizar **Bitcoin** como herramienta de inversión, es crucial enfocarlo con una mentalidad a largo plazo y centrarse en sus principios fundamentales de descentralización y soberanía financiera. Esta sección proporcionará información sobre los riesgos y beneficios de invertir en **Bitcoin**, así como consejos prácticos para comprar, mantener y utilizar **Bitcoin** para su propósito previsto como un depósito de valor descentralizado y seguro.

Los "*tendencias del mercado*" se refieren a la **dirección** general en la que se mueve el mercado. Una tendencia alcista es cuando el mercado está en una trayectoria ascendente, mientras que una tendencia bajista es cuando el mercado está en una trayectoria descendente. Esto suele estar asociado con el optimismo de los inversores y la expectativa de que los precios seguirán aumentando. En cambio, una tendencia bajista es cuando el mercado está en una trayectoria descendente, caracterizada por máximos y mínimos más bajos. Esto suele estar asociado con el pesimismo de los inversores y la expectativa de que los precios seguirán cayendo.

El análisis técnico no es una ciencia perfecta y el rendimiento pasado no siempre es indicativo de resultados futuros. Debe usarse en conjunto con otras formas de análisis, como el análisis fundamental y el sentimiento del mercado, para tomar decisiones informadas de trading e inversión.

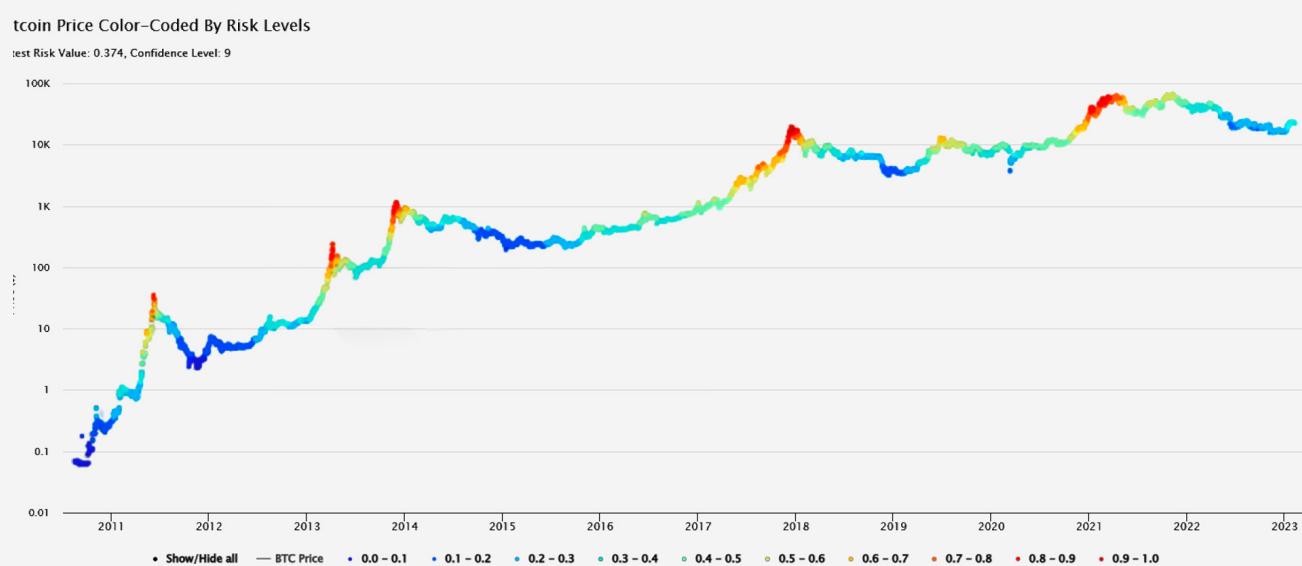
La "*carta de métrica de riesgo*", creada por Benjamin Cohen, es una forma rápida e intuitiva de comprender el sentimiento del mercado y evaluar posibles oportunidades de compra o venta para el **bitcoin**. Esta carta muestra el precio de los activos y asigna un valor codificado por colores para representar el riesgo asociado con ese precio. Los valores de riesgo van del 0 al 1, siendo los colores rojos oscuros los que indican un mayor riesgo y los colores azules oscuros los que indican un menor riesgo.

El propósito de la métrica de riesgo no es predecir los máximos o mínimos del mercado, sino identificar áreas que puedan ser atractivas para comprar o vender a largo plazo. Una puntuación de bajo riesgo sugiere que el **bitcoin** puede estar subvalorado y puede presentar una oportunidad de compra, mientras que una puntuación de alto riesgo sugiere que puede estar sobrevalorado y puede presentar una oportunidad de venta.

## Información Adicional

### Color del Precio de Bitcoin – Codificado por Niveles de Riesgo

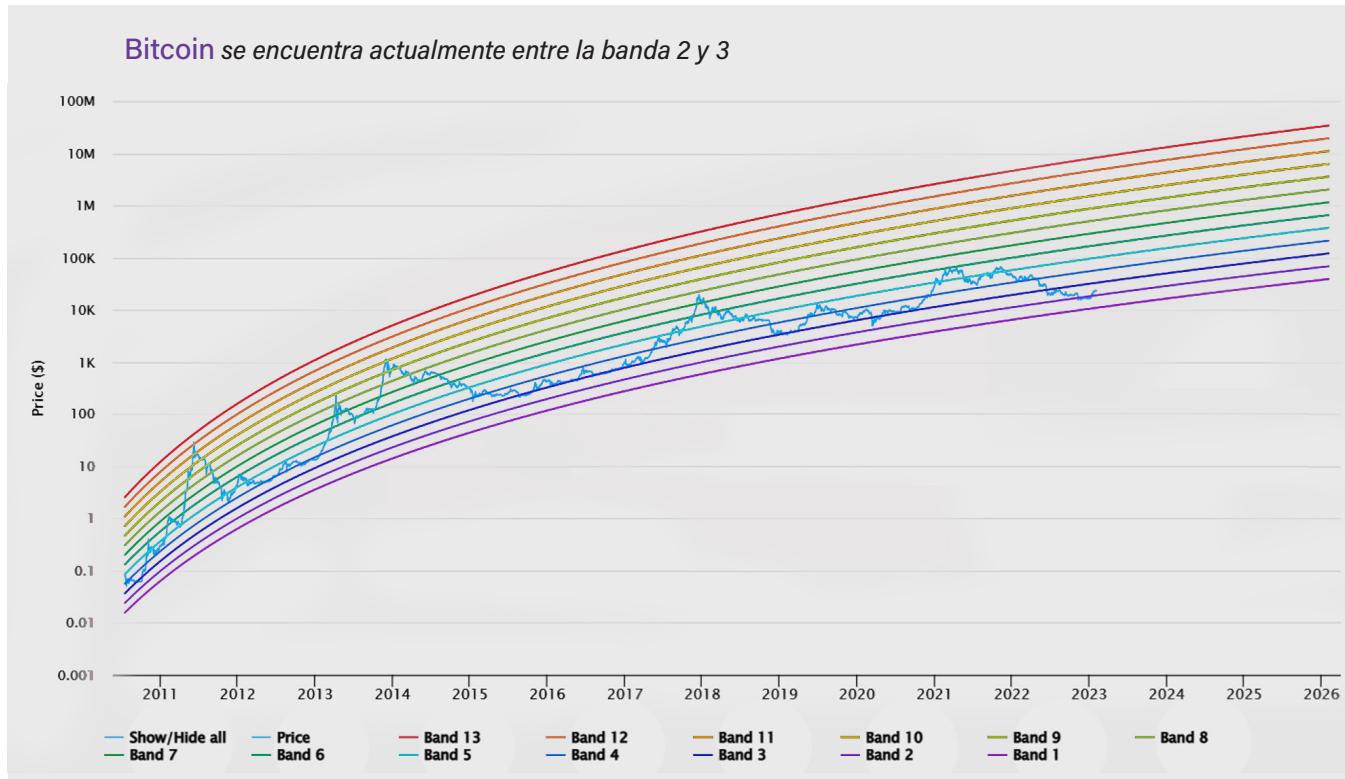
Último Valor de Riesgo: 0,374, Nivel de Confianza: 9



El “*precio de mercado logarítmico*” es un método para visualizar los movimientos de precios de un activo, como el **bitcoin**, a lo largo del tiempo. Este enfoque utiliza una escala logarítmica en el eje y para reflejar mejor el crecimiento exponencial que a menudo se ve en los precios de los activos.

El precio de mercado logarítmico se utiliza para rastrear los movimientos de precios del **bitcoin** a lo largo del tiempo y para identificar posibles picos y zonas de acumulación. Los ciclos de mercado mencionados en el ejemplo son períodos de aumento y disminución de precios, y las bandas arco iris se utilizan para ilustrar la magnitud relativa de estos movimientos de precios.

El precio de mercado logarítmico puede ser útil para identificar zonas potenciales de acumulación, o períodos en los que el precio puede estar relativamente bajo y brindar una buena oportunidad de compra. En el ejemplo, las zonas entre la banda 3 y la 4 se identifican como buenos períodos de acumulación para los ciclos de mercado 3 y 4.



**Los Ciclos de Mercado** en Bitcoin se refieren al patrón recurrente de crecimiento y contracción en su precio y actividad del mercado. Se caracterizan por períodos de especulación y exageración, seguidos de correcciones y consolidación. Algunos analistas argumentan que los ciclos están fuertemente correlacionados con los eventos de halving.

Es importante tener en cuenta que aunque el precio de mercado logarítmico puede proporcionar información valiosa, es solo una de las muchas herramientas que se pueden utilizar para analizar las tendencias del mercado y los movimientos de precios, y se debe utilizar en conjunto con otros métodos de análisis para formar una comprensión más completa del mercado. Además, las condiciones del mercado están cambiando constantemente, y el rendimiento pasado no es una garantía de resultados futuros.

**La relación Hash/Precio** y la relación Precio/Hash son métricas utilizadas para comparar el crecimiento del precio de bitcoin y el crecimiento de la potencia informática de la red Bitcoin, o la tasa de hash. Estas métricas se utilizan para ayudar a comprender la relación entre ambas y cómo los cambios en una pueden afectar a la otra.

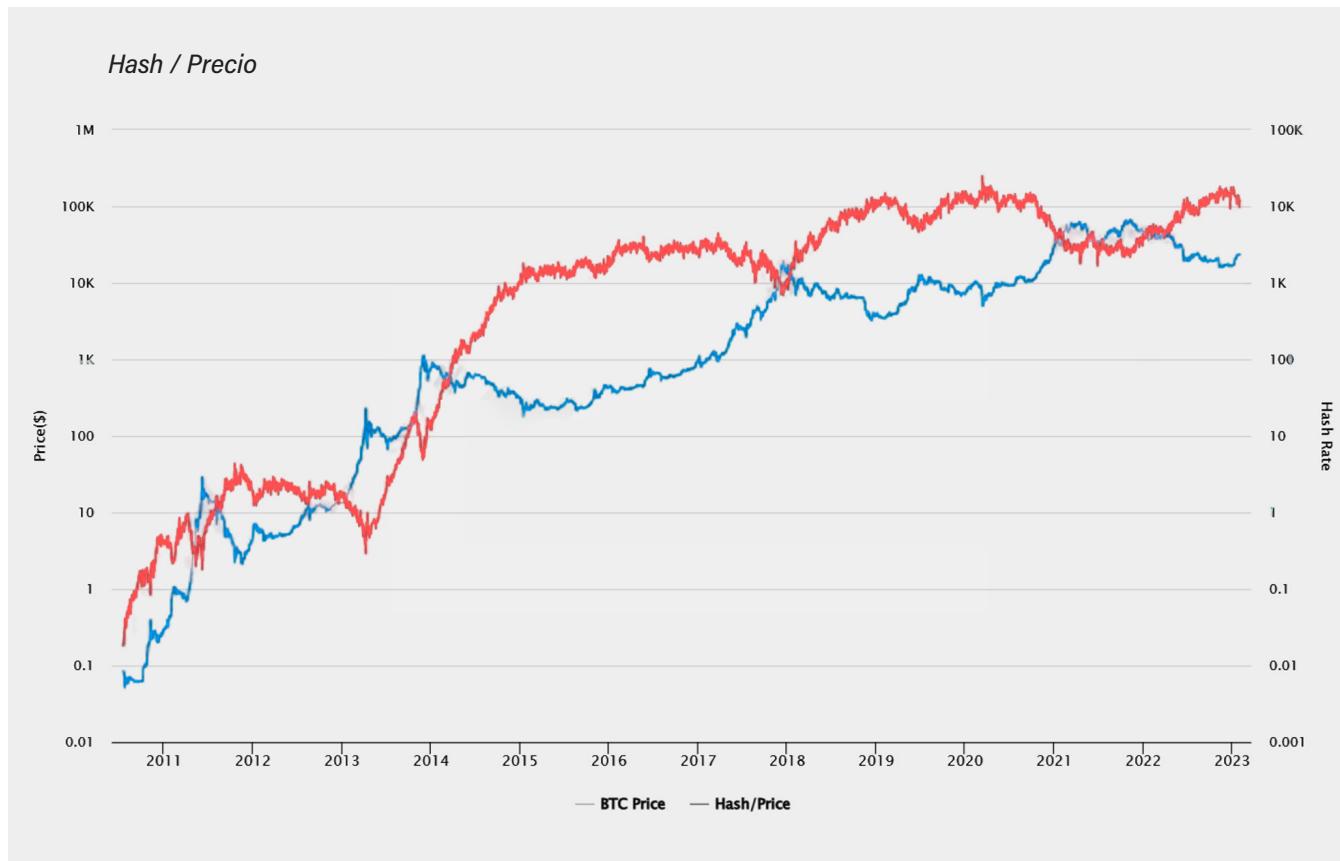
Cuando el precio de bitcoin aumenta a un ritmo más rápido que la tasa de hash, la relación Hash/Precio disminuye y la relación Precio/Hash aumenta. Esto significa que el precio de bitcoin está creciendo más rápido que la potencia informática de la red, lo que podría indicar un aumento de la demanda de bitcoin.

## Información Adicional

Sin embargo, cerca de los picos locales, cuando el precio de **bitcoin** está aumentando rápidamente, puede haber caídas repentinas en la relación Hash/Precio. Esto se debe a que el crecimiento en el precio supera el crecimiento en la potencia informática, lo que conduce a una disminución en la relación Hash/Precio.

Por otro lado, si tanto la tasa de hash como el precio de **bitcoin** disminuyen o aumentan a las mismas tasas relativas, las relaciones se mantendrán constantes. Esto significa que la potencia informática de la red y el precio de **bitcoin** están creciendo al mismo ritmo.

Si la tasa de hash de la **red Bitcoin** está aumentando a un ritmo más rápido que el precio de **bitcoin**, la relación Hash/Precio aumentará y la relación Precio/Hash disminuirá. Esto podría indicar que la red se está volviendo más segura y más capaz de procesar **transacciones**, lo que podría tener un impacto positivo en el precio de **bitcoin** en el futuro.



Las **Líneas de tendencia** se utilizan para identificar la tendencia actual del mercado. Se forman conectando dos o más puntos de precio y se utilizan para indicar un nivel de soporte o resistencia. Una línea de tendencia que se inclina hacia arriba se considera alcista, mientras que una que se inclina hacia abajo se considera bajista.

Las **medias móviles** se utilizan para suavizar la volatilidad del precio de un valor durante un período específico de tiempo. Se calculan sumando los precios de cierre de un valor durante un número específico de períodos y

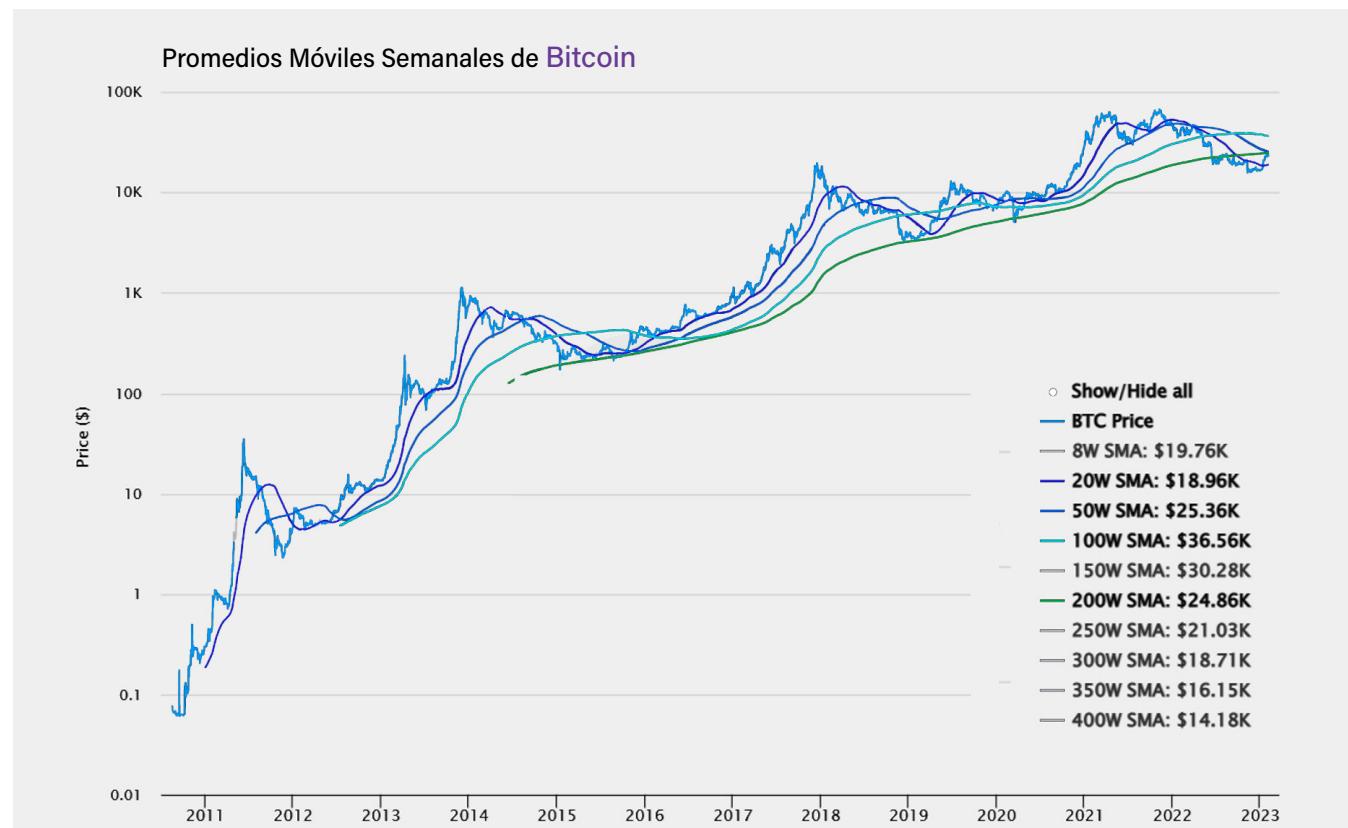


luego dividiendo por el número de períodos. Una media móvil se puede utilizar para identificar la dirección de una tendencia y también se puede utilizar para generar señales de compra y venta. *El promedio de costo en dólares* (DCAing) por debajo de las medias móviles a corto plazo como el SMA de 100 semanas y el SMA de 50 semanas puede proporcionar más puntos de entrada, pero puede dejarlo con pérdidas a corto plazo.

El objetivo del DCA es reducir el impacto de la volatilidad del mercado en una cartera de inversión distribuyendo las compras en el tiempo, en lugar de comprar todo de una sola vez.



*El promedio de costo en dólares (Dollar-cost averaging, DCA)* es una estrategia de inversión que consiste en invertir una cantidad fija de dinero en un activo en particular a intervalos regulares, independientemente del precio.



- Por ejemplo, un inversor puede decidir invertir \$100 en **bitcoin** cada mes. Si el precio es alto, el inversor comprará menos unidades, y si el precio es bajo, el inversor comprará más unidades. Con el tiempo, este enfoque puede conducir a un costo promedio más bajo por unidad, y así reducir el impacto de las fluctuaciones de precios a corto plazo.

El **DCA** se puede utilizar en una variedad de inversiones, incluyendo acciones, bonos y materias primas, y se recomienda a menudo para personas que están empezando a invertir y quieren minimizar el riesgo de la volatilidad del mercado.

Es importante tener en cuenta que el DCA no garantiza una ganancia ni protege contra la pérdida en un mercado en declive, y debe combinarse con una investigación exhaustiva y análisis del mercado. Además, los inversores deben considerar sus propios objetivos financieros y tolerancia al riesgo al decidir la mejor estrategia de inversión.

Los indicadores **RSI** y **MACD** son herramientas que se utilizan para analizar los mercados financieros y pueden ayudar a los inversores a identificar oportunidades de compra o venta de cualquier tipo de activos, incluyendo **bitcoin**.

El **RSI** compara las ganancias y las pérdidas recientes de un activo para determinar si está sobrecomprado (ha subido demasiado y puede haber una corrección a la baja) o sobrevenido (ha caído demasiado y puede haber una corrección al alza).

Por otro lado, el **MACD** se calcula al restar la media móvil exponencial (EMA) de 26 períodos de la EMA de 12 períodos y luego se traza una EMA de 9 días del resultado. Este indicador se utiliza para identificar cambios en la **dirección** del impulso y de la tendencia de un activo.

La inversión y el trading en **bitcoin** pueden ser una actividad emocionante y potencialmente lucrativa, pero es importante recordar que se trata de una actividad de alto riesgo que requiere una comprensión profunda del mercado y una actitud a largo plazo. Los inversores deben utilizar herramientas de análisis técnico y fundamental para tomar decisiones de inversión informadas y tener en cuenta su propio perfil de riesgo y objetivos financieros antes de invertir en **Bitcoin** o cualquier otra criptomoneda. Además, siempre se debe tener en cuenta que el rendimiento pasado no garantiza resultados futuros, ya que las condiciones del mercado pueden cambiar rápidamente. Por lo tanto, la inversión en **Bitcoin** debe ser abordada con prudencia y una gestión cuidadosa del riesgo.











