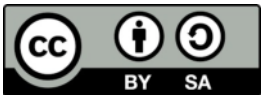
Mi Primer Bitcoin
EL SALVADOR

Diplomado en Bitcoin

EDUCACIÓN FINANCIERA BASADA EN BITCOIN

Libro de Trabajo para Estudiantes

Tercera Edición | Septiembre 2022



Diplomado en Bitcoin

EDUCACIÓN FINANCIERA BASADA EN BITCOIN

Libro de Trabajo para Estudiantes

Tercera Edición | Septiembre 2022

PARA DONAR:

Mi Primer Bitcoin
EL SALVADOR

bc1qc0h5ddd4ln4z05u55l87cp4umg8eg0jjkhcgvf

Agradecimientos

El ***Diplomado en Bitcoin*** ha sido un éxito rotundo y ha crecido más rápido de lo que nos hubiésemos podido imaginar. Nos gustaría dar crédito a todas aquellas personas maravillosas que nos han traído hasta aquí.

El equipo central del plan de estudios, la fuerza impulsora de este contenido es Dalia Platt, Gloriana Solano, Raúl Guirola y Robert Malka. Han trabajado incansablemente detrás del escenario durante meses, primero para crear esto con una seria escasez de tiempo y luego para seguir aprendiendo y mejorando. Sin estos cuatro, nada de esto habría sido posible. A lo largo del camino, ese grupo central ha contado con la ayuda de Giacomo Zucco, Pedro Solimano, María Andrée Maegli, Alejandro Machado, Gerson Martínez y Vriti Saraf. Gerardo Apóstolo y Enrique Jubis, diseñadores de ACTIVA, también hicieron un trabajo increíble.

La historia del ***Diplomado en Bitcoin*** comienza en febrero del 2022 en una reunión en La Pacheco, una escuela pública en San Marcos, El Salvador. Nos movimos rápido, recaudamos fondos de más de 400 donantes individuales, comenzamos las clases en abril y graduamos al primer grupo en junio.

Los arquitectos de aquella reunión de febrero son también personajes imprescindibles en esta historia. El director de La Pacheco, Asael Rodríguez, estaba dedicado a preparar a sus alumnos para un mundo cambiante. El diputado Rodrigo Ayala, que ya apoyaba a La Pacheco, también reconoció la necesidad de la educación de Bitcoin. Carlos Toriello, creador de comunidades en IBEX Mercado, invitó a otros Bitcoiners, incluyéndome a mí, a venir a ver la escuela y conocer el plan de estudios.

Carlos e IBEX merecen su propia sección aquí. Ellos pusieron los fondos para que La Pacheco construyera una nueva cafetería, defendieron la causa, nos ayudaron a financiar el resto de los gastos y organizaron a gente de todo el mundo para que participara y fuera testigo de la primera promoción. El ***Diplomado en Bitcoin*** ahora existe en otros lugares y con otros patrocinadores, pero está construido a base del éxito del programa piloto en La Pacheco, y simplemente no habría ocurrido sin ellos.

Mi Primer Bitcoin es una organización sin fines de lucro con una misión singular: *brindar educación de calidad e imparcial sobre Bitcoin a todos en El Salvador, y luego a todos en el mundo*. Como la primera nación en adoptar Bitcoin, creemos que El Salvador puede ser un ejemplo de base. Nuestra visión es enseñar a una nación y cambiar el mundo. Sé que suena loco, pero creo que estamos en camino y el ***Diplomado en Bitcoin*** es una gran parte de eso.

Por un mundo mejor,

John Dennehy

Fundador
Mi Primer Bitcoin

Índice

Clase #6-

Clase #7 -

Clase #8 -

Clase #9 -

Clase #10 -

Clase Adicional -

¿Por qué Bitcoin?

Ejercicio Práctico. Escribe abajo por qué crees que es importante aprender sobre **Bitcoin**. No hay respuesta incorrecta.

Clase #1

Introducción: El Sistema Monetario

1.1 Actividad: Introducción al Dinero
1.2 ¿Qué problemas existen con el dinero de hoy?
- Consecuencias del Desarrollo
  - Necesidades vs. Recursos
- La Modernización

1.3 Definición del Dinero
- Funciones del Dinero
- Características del Dinero
- Dinero Convencional y Activo Monetario
  - Tipos de Dinero
  - Actividad: ¿Son las pasas un buen dinero?

Introducción: El Sistema Monetario

1.1 Actividad: Introducción al Dinero

Actividad de Clase. Espera instrucciones del maestro para realizar esta actividad.

1.2 ¿Qué problemas existen con el dinero de hoy?

Estamos programados para resistir los desafíos de la vida y progresar. Es un proceso humano natural el querer superarnos, llevar una vida productiva, creativa y valiosa, pero:

- Vivimos en un mundo donde hay mucho para pocos, y muy poco para muchos.
  - Los individuos de menores recursos económicos no cuentan con las mismas oportunidades. ¿Porqué?
    - No tienen acceso a los mismos niveles de educación.
    - No pueden acceder a los créditos necesarios para comenzar sus negocios.

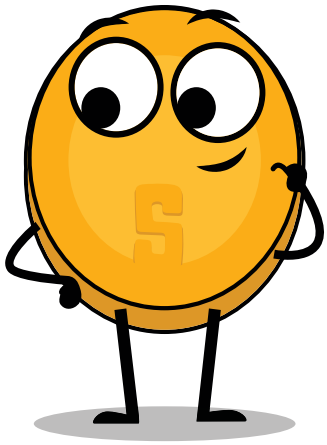
- Para reducir la pobreza y estimular el bienestar social, es importante:
  - Mejorar el acceso a la educación financiera para todos.
  - Desarrollar la capacidad de administrar dinero.
  - Aprender a utilizar nuevas tecnologías de manera responsable.
  - Planear para el futuro.

Veremos que **Bitcoin** es una herramienta y un tipo de dinero:

- Transparente, descentralizado, global, digital, barato, privado, programable, de fácil y rápido acceso, que puede ayudar a remediar estos problemas.

SATOSHI

Él es *SATOSHI*, un asistente interactivo que te ayudará durante todo el *Diplomado en Bitcoin*. *SATOSHI* te dará datos y recomendaciones para entender mejor.



Consecuencias del Desarrollo

- Las personas siempre han necesitado alguien que financie sus aspiraciones futuras.
  - Formas de intercambiar salarios, tiempo, y energía por depósitos de valor.

- Si no hubiésemos evolucionado, habríamos quedado reducidos a una *economía de trueque*.
  - Cada cosa que alguien quisiera comprar tendría que ser canjeada por algo que esa persona pudiera proveer.

- El desarrollo permanente ha revolucionado las sociedades y la interacción global. En general, con un interés común de mejorar la calidad de vida de futuras civilizaciones.
  - A medida que la tecnología avanza y aumenta la productividad, deberíamos:
    - *Bajar los precios de forma natural.*
    - *Fortalecerse la moneda*
    - *Poder comprar más por menos.*
  - Pero sucede lo contrario:
    - *Los precios suben, las monedas se debilitan y compramos menos por más.*

— ¿Cómo hemos llegado hasta aquí?

— ¿Cómo, porqué, y para qué se crea más dinero y cuales son las consecuencias?

— ¿Qué hay escondido tras los sistemas financieros hoy?

— ¿Cuál es el peligro invisible de la pérdida de valor del dinero?

— ¿Cómo podemos darle valor adicional a nuestros ahorros?

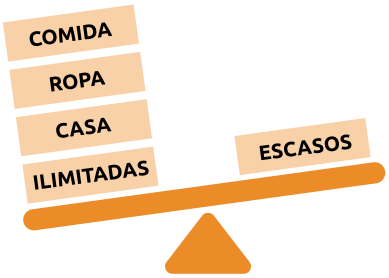
- Hoy, sólo los bancos y los gobiernos tienen el poder de emitir dinero en una economía.

El dinero simplemente no se acaba. Los gobiernos imprimen la cantidad de dinero necesaria para financiar sus gastos públicos, inyectar recursos en la economía y retirarlos después en forma de impuestos.

- El problema es que como humanidad, gastamos más de lo que generamos. Como consecuencia tenemos:
  - Pérdida de confianza en el valor del dinero y en el sistema bancario moderno.
  - Inestabilidad económica y política mundial e incluso, trae guerras.
    - ¿Porqué?

Necesidades vs. Recursos

Nuestras necesidades son infinitas pero nuestros recursos escasos.

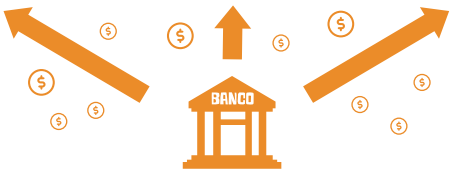


La Modernización

"Se debe confiar en los bancos para que retengan nuestro dinero y lo transfieran electrónicamente, pero lo prestan en oleadas de burbujas crediticias con apenas una fracción en reserva."

–Satoshi Nakamoto

La administración pública, las empresas y muchas familias necesitan dinero y se lo piden al banco. Pagan intereses por esas deudas.



El banco es un intermediario. Es decir, compra el dinero de los ahorradores y se lo vende a quien lo necesita, a un interés mayor.

Muchas familias ahorran. Depositan su dinero en el banco, y cobran un pequeño interés.

Introducción: El Sistema Monetario

El negocio bancario consiste en:

- La compra de dinero en forma de depósitos de los ahorradores, y su posterior venta mediante préstamos a aquellos que lo necesitan.

- Su beneficio, como en cualquier otro negocio, proviene de:
  - Un mayor precio de venta que el de compra- la tasa de interés del dinero que presta es mayor a lWa que paga a los ahorradores.
  - Pero la clave del poder bancario reside en la posibilidad de- vender algo que no es de su propiedad, sino del ahorrador correspondiente.

- Los gobiernos controlan la emisión de sus monedas- intentan solucionar ciclos económicos problemáticos.

- Las economías imprimen más dinero en momentos de recesión
  - Estimulan el crecimiento a corto plazo.
  - Reducen el desempleo a corto plazo.

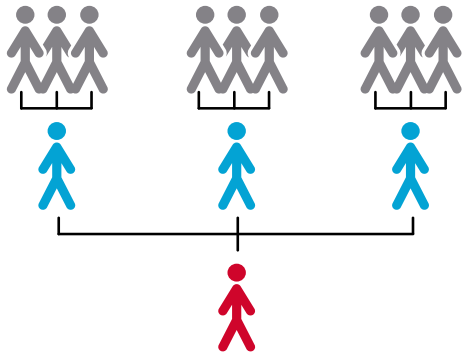
- La necesidad del papel moneda físico ha perdido su importancia.
  - La banca por internet ha facilitado el uso del crédito.

Los Beneficios

— Facilitan transacciones inmediatas y planeación hacia el futuro.
— Registran todos los movimientos de los ahorradores y deudores en bases de datos centralizadas.
— Actualizan constantemente las salidas y entradas de sus usuarios.
— Verifican la legitimidad de las cuentas.
— Si el dinero desaparece en una cuenta por una de múltiples razones, es reemplazable.
— Cuentan con pólizas de seguro en caso de ser víctimas de un robo.

Los Costos

— El sistema bancario tiene una única fuente de falla, es centralizado y se puede manipular fácilmente.



— Los gobiernos pueden:
  - Expandir y contraer libremente la oferta monetaria.
  - Confiscar cuentas bancarias.
  - Bloquear retiros sin previo aviso.
  - Enfrentar graves problemas técnicos o piratería informática.
  - Eliminar algunos servicios básicos.
  - Maniobrar las tasas de intereses y los impuestos.

— La inflación alta y las tasas de interés negativas causan que el valor del dinero baje.

"Un banco es un lugar en el que prestan a usted un paraguas cuando hace buen tiempo y se lo piden cuando empieza a llover."

- Robert Lee Frost

1.3 Definición del Dinero

Aceptamos pagos en efectivo, transferencias, cheque y/o tarjeta de crédito a cambio de bienes y/o servicios.

• **No** nos detenemos a pensar que todos estos medios de intercambio son únicamente promesas de pago.

Alguna vez te has preguntado, ¿qué es el dinero? En este video veremos una reflexión sobre esto.

— SATOSHI

Funciones del Dinero

El dinero cumple **tres funciones**:

1. Depósito de valor que se puede invertir, ahorrar, solicitar o prestar.
2. Medio de intercambio para pagar bienes y servicios.
3. Unidad de medida que permite comparar los precios entre productos.

▫ **Depósito de Valor**. Tiende a mantener su valor a través del tiempo.

▫ **Medio de Intercambio.** Elimina el complejo sistema de trueque permitiendo el intercambio de bienes y el pago de deudas con mayor eficiencia.

▫ **Unidad de Medida.** Permite que exista un patrón universal de un sistema de precios para expresar el valor de bienes y servicios.

Ejercicio Práctico. Escribe el nombre de la función del dinero correcta.

_____ . El dinero facilita el intercambio porque todo el mundo lo acepta como pago.

_____ . El dinero ayuda a mantener la riqueza, ya que nos permite ahorrar y poder gastarlo en un futuro.

_____ . El dinero permite medir el valor de los bienes y servicios y hacer comparaciones entre bienes diferentes. Una etiqueta con precio caro nos dice algo sobre el valor del bien.

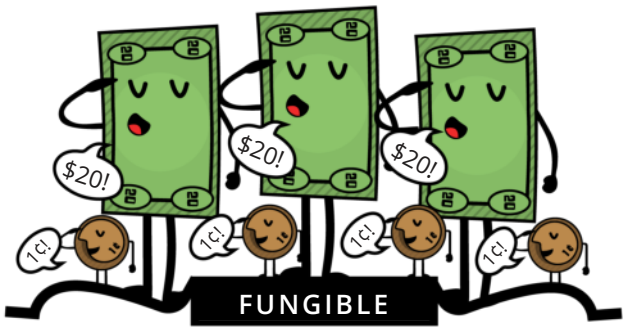
Introducción: El Sistema Monetario

Características del Dinero

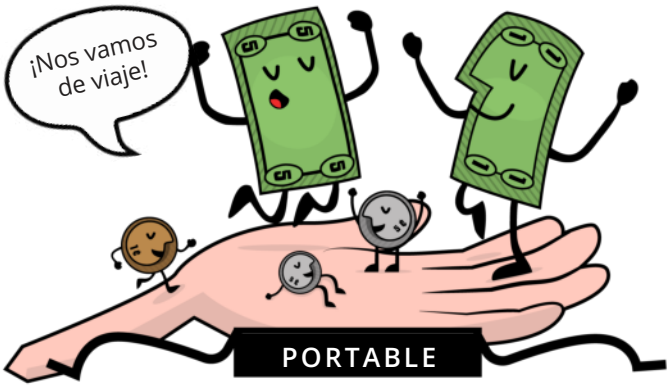
El dinero puede tomar muchas formas. Entre más de estas características demuestra un tipo de dinero, mejor dinero es.

- **Durabilidad**. El dinero debe resistir el deterioro físico y perdurar en el tiempo. Debe ser capaz de circular en la economía en un estado aceptable y reconocible.

- **Uniformidad o Fungibilidad.** Cada unidad de dinero debe ser exactamente igual a cualquier otra.



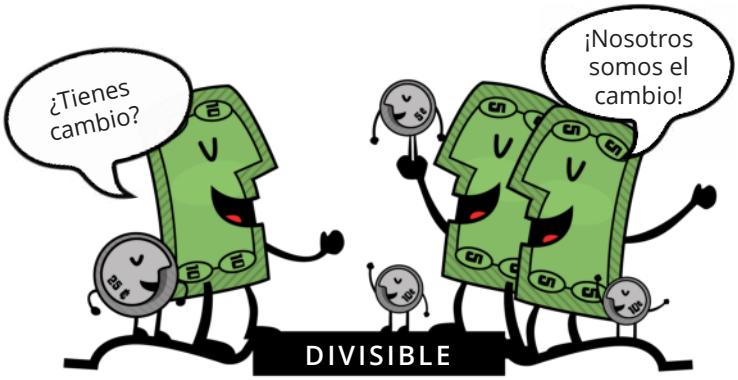
- **Portabilidad**. Tiene que ser fácil de trasladar de un lado a otro. Debe poder acumular mucho valor en poco peso.



- **Reconocibilidad o Aceptabilidad.** El bien que se utilice tiene que ser reconocido por todos como dinero.

- **Escasez.** El valor del dinero depende de la oferta y la demanda. Mientras más dinero se ofrezca y menos se necesite, su valor será menor.

- **Divisibilidad**. Debe servir para adquirir bienes caros y baratos y ser fraccionado sin perder su valor.



Dinero Convencional y Activos Monetarios

- El **Dinero Convencional** es el dinero de uso general en un país en particular.
  - Efectivo en circulación, depósitos bancarios y reservas del banco central.
  - La mayoría es crédito o entradas electrónicas en los libros contables.
  - **No necesariamente** guarda su **valor** en el **tiempo**.

- Los **Activos Monetarios** generalmente **sí** guardan su **valor** en el **tiempo**.

Tipos de Dinero

- **Dinero Mercancía**
  - Difíciles de extraer, escasos.
  - Atractivos como reserva de valor.
  - El oro y la plata perduraron como buen dinero durante miles de años.

  — [Activo Monetario]

- **Representativo**
  - Billetes respaldados en oro o plata.
  - Cada billete se intercambia por su valor equivalente en metal.
  - En la historia moderna, el patrón oro duró hasta 1971.

  — [Activo Monetario inicialmente, pero se convierte en Dinero Convencional al pasar del tiempo- si se incrementa la oferta monetaria].

- **Fiat o Moneda Fiduciaria**
  - Implementada como monopolio y emitida a voluntad por un gobierno.
  - No está respaldada por un producto físico.
  - No tiene valor intrínseco; su valor depende de:
    - La relación entre oferta y demanda.
    - La estabilidad del gobierno emisor.

  — [Dinero Convencional. El fiat digital tiene más riesgo de contraparte que el físico].

- **Bitcoin**
  - Moneda digital escasa.
  - Opera de manera descentralizada.
  - Se basa en software y criptografía "*persona a persona*" para realizar movimientos.

  — [Activo Monetario]

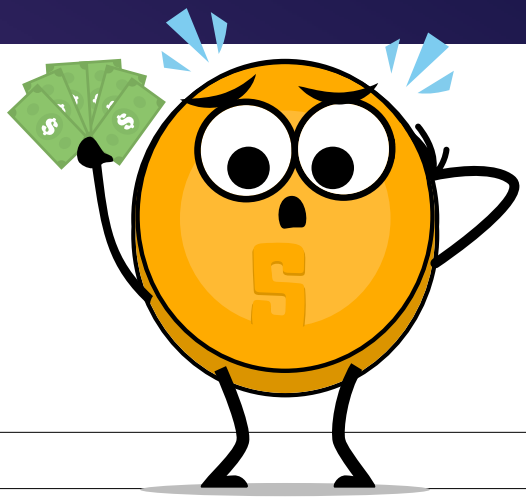
Introducción: El Sistema Monetario

Ejercicio Práctico. Marca con una **X** si el artículo cumple con la característica indicada. ***¿Cuál artículo escogerías como dinero?*** ** No llenes la última columna 'Bitcoin' hasta después de completar la Clase #4.*

Característica	 Manzanas	 Conchas	 1oz. Oro	 1 USD	 Bitcoin
Uniforme o Fungible					
Divisible					
Portable					
Escaso					
Durable					
Reconocible					

¿Cuál artículo escogerías como dinero?

Actividad: ¿Son las pasas un buen dinero?



Actividad de Clase. Espera instrucciones del maestro para realizar esta actividad.

Clase #2

Historia, Evolución y Devaluación del Dinero

Historia, Evolución y Devaluación del Dinero

2.1 Historia del Dinero

El dinero es algo que usamos a diario, pero rara vez paramos a pensar... ¿de dónde vino? ¿cómo transaban nuestros ancestros?

- Lo que ha constituido dinero, ha variado a través del tiempo y de un lugar a otro.

- El dinero es tan antiguo como el lenguaje mismo. Es simplemente una forma de comunicación, una tecnología.

- No existe un acuerdo universal sobre lo que realmente es.

- En principio, no necesitaríamos un activo especial como un billete para reconocer a quién se le deben bienes y/o servicios.
    - Cualquier persona podría tener su propio libro contable.
    - Nuestros ancestros transaban de esta forma y/o a través del trueque sin necesidad de bancos o dinero convencional.

2.2 Actividad: Juego del Trueque

Volvamos al Pasado: El Trueque

Para producir el trueque debe existir una doble **coincidencia de necesidades**.

- Una persona que quiere intercambiar algo necesita encontrar un socio comercial que tenga lo que quiere y quiera lo que tiene.

- Este medio de intercambio de bienes y servicios requiere mucho tiempo, restringe la actividad económica y limita la especialización.

- El dinero alivia estos problemas.

Actividad de Clase. Espera instrucciones del maestro para realizar esta actividad.

1. ¿Qué es el trueque?

2. ¿Cuáles son los problemas principales con el trueque?

3. ¿Qué es el dinero mercancía?

4. ¿Qué problemas surgen cuando se utiliza el dinero mercancía?

5. ¿Qué es el dinero?

6. ¿Por qué la gente está dispuesta a aceptar dinero?

Historia, Evolución y Devaluación del Dinero

2.3 Evolución del Dinero en el Tiempo

El intercambio de bienes materiales o de servicios por otros — es — EL TRUEQUE

Donde el dinero no intermedia

Evolución del Dinero en el Tiempo — surgió — Como una necesidad de la comunidad y de las estructuras sociopolíticas.

Dinero ≠ Unidades Monetarias

DINERO MERCANCÍA

Un bien representaba el dinero

el cual tenía

valor intrínseco y **valor de uso**

cumplía las características de

- ser aceptada como medio de pago
- medida de valor

se utilizaban

- Sal
- Cacao
- Ganado

DINERO METÁLICO

El dinero se expresaba

en

monedas y **especies metálicas**

se caracterizaban por ser

- fácil de transportar
- dividible
- almacenable

Se acuñaron las primeras monedas

- Oro
- Plata
- Cobre

DINERO PAPEL

La emisión de documentos respaldados

por

metales preciosos (que son aceptados por todos)

se caracterizaban por ser

- fácil de transportar
- dividible
- respaldo total del gobierno

DINERO FIDUCIARIO

Está respaldado por la ***confianza*** de una sociedad

no se basa en el valor

sino

en la creencia general que dicho dinero tiene valor

lo cual llevó

creación de Bancos Centrales

Monopolio Autoritario

DINERO PLÁSTICO

Creación del sistema de tarjetas de crédito y débito.

así como

- monederos electrónicos
- tarjetas

funciona como

transacciones bancarias (prestando un valor sustituto al dinero en efectivo)

CRIPTOMONEDA

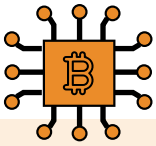
Un medio digital de intercambio que utiliza la criptografía fuerte para asegurar

- transacciones
- creación de unidades
- verificar la transferencia de activos

son independientes a los bancos

su valor depende de

- Usabilidad
- Suministro
- Demanda



El Patrón Monetario Internacional en la Historia

Patrón Bimetálico (s. XVII-XIX)
Los billetes podían convertirse en oro y plata.

Patrón Oro (1870 - I Guerra Mundial)
Cualquier ciudadano podía convertir su papel moneda en una cantidad de oro prefijada.

Período de Entreguerras
Las dos guerras y la crisis de 1929 acabaron con la convertibilidad en oro para los particulares.

Pacto de Bretton-Woods
Al finalizar la II Guerra Mundial, en 1945, los aliados establecieron que las monedas eran convertibles en dólares estadounidenses.

Crisis de los 70's
En 1971, la situación económica estadounidense, unida a la Guerra de Vietnam, provocó que los BCE's traten de convertir sus dólares en oro, lo que creó una crisis en E.E.U.U. e hizo que Nixon suspendiera la convertibilidad del dólar en oro.

Etapa Actual
Desde 1973, hasta hoy, el dinero es dinero fiduciario y digital.

- El dinero ha evolucionado a lo largo de la historia, enfrentando desafíos y cambios de necesidades.
    - Normalmente, se eligió la forma de dinero que ofrecía las características superiores.
    - Pero desde que se empezaron a recortar las monedas y la transición de metales preciosos a metales respaldados por papel:
        - Pasamos de una selección natural de la forma de dinero con mejor rendimiento, a una de facilidad de uso, mayor portabilidad y divisibilidad.
    - Hubo un giro hacia la centralización.

2.4 Cambio Repentino al Fiat

La época industrial marcó el inicio de la centralización:

- El objetivo era distribuir correctamente los bienes producidos.
    - Se crearon los Bancos Centrales.
    - Nació el sistema de tarjetas de crédito y débito.

- Cuando el dinero se centraliza, pueden ocurrir problemas profundos.
    - Los gobierno monitorean de cerca la actividad económica de sus ciudadanos.
    - El abuso de poder puede llevar a:
        - Estímulos económicos e intervenciones gubernamentales.
        - Explosión de deuda y consumo irresponsable.
        - Aumento en la desigualdad de riqueza.

Hasta 1971, se usaba dinero representativo: *medio de intercambio* y *reserva de valor.*

- A partir 1971, nos alejamos del dinero sólido hacia un mundo basado en la deuda.
    - Richard Nixon, eliminó la libre convertibilidad del oro por el dinero.
    - Pasamos al experimento actual, que es el ***dinero fiat***.
    - El dinero moderno es por decreto y no por consenso.
    - ***Fiat*** viene del latín y significa por decreto: es elegido y establecido por ley.

"Aquello que funcionó ayer, no necesariamente funcionará hoy."

- Jordan Peterson

2.5 Los Bancos Centrales

- El objetivo y la función de un ***Banco Central***:
  - Controlar la política monetaria del país con el fin de garantizar estabilidad.
  - Su función es ser el banquero de los bancos.
  - Su trabajo principal: manipular la oferta del dinero en circulación.
    - Controlar la inflación y maximizar el empleo a con políticas económicas y financieras.
  - El Banco Central de los E.E.U.U. se llama *la Reserva Federal*.

La Reserva Federal ha recibido un doble mandato:

- ¿Quién define y quién se beneficia de estos objetivos?
  - Los grandes bancos- pueden influenciar las políticas federales, e incluso globales.

- ¿Cómo altera la oferta monetaria la Reserva Federal?
  - A través del sistema bancario de **reserva fraccionaria**.
  - Los bancos en E.E.U.U. sólo mantienen un 10% de sus depósitos en reserva.
  - La banca de reserva fraccionaria resulta en un **multiplicador bancario**.
    - *Más de dos personas usan el mismo dinero a la vez en la economía de un país.*

> *Los bancos tienen la obligación de mantener un cierto porcentaje de todos los depósitos en el banco. Reducir ese porcentaje significa que puede circular más dinero, y aumentarlo significa que circula menos dinero.*

- ¿Qué problemas puede provocar la banca de **reserva fraccionaria**?
  - Los bancos "piden prestado y prestan a largo plazo".
    - El retiro de depósitos excede las reservas de efectivo.
    - Los bancos incurren grandes pérdidas.
    - En los peores de los casos se produce una corrida bancaria.
  - Los cambios en las tasas de interés o el costo del capital afectan el riesgo.
    - Más dinero en circulación significa préstamos más baratos y menos exigentes.

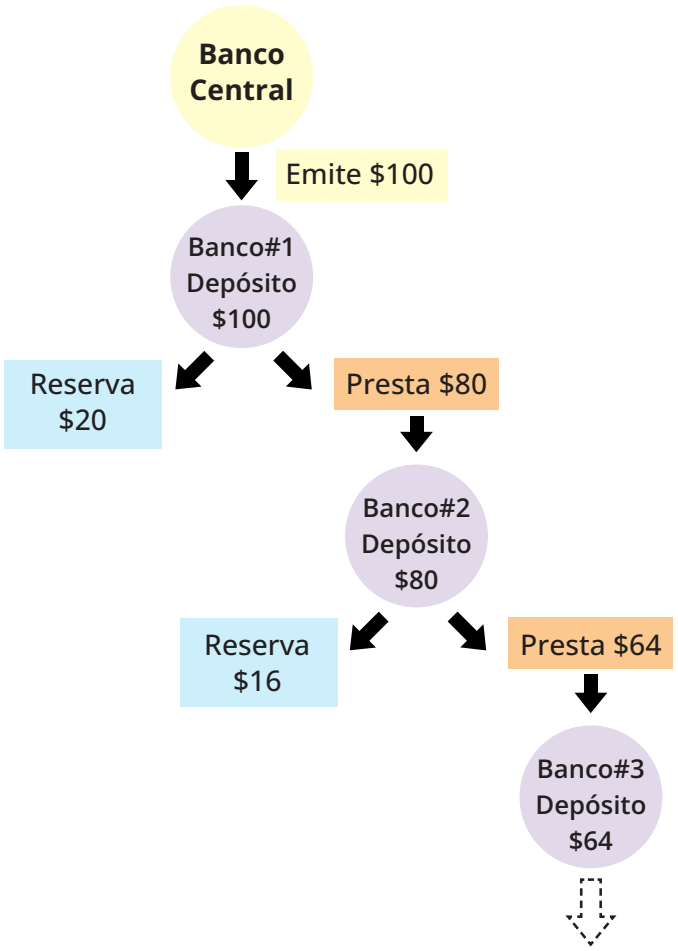
- Operaciones de mercado abierto (*para aumentar o disminuir el dinero en circulación*).
  - El gobierno compra o vende títulos monetarios (deuda de alta liquidez).
    - Si quieren aumentarlo: *compran* bonos de la tesorería.
    - Si quieren disminuirlo: *venden* bonos de la tesorería.

2.6 Actividad: Reserva Fraccionaria

Actividad de Clase. Espera instrucciones del maestro para realizar esta actividad.

REGISTRO BANCARIO

	Dólares de Préstamo	Depósito de Dólares	Requisito de Reserva del 10%
Depositante A			
Prestatario A			
Depositante B			
Total Dólares			



Clase #3

Los Efectos del Dinero Fiat y la Centralización

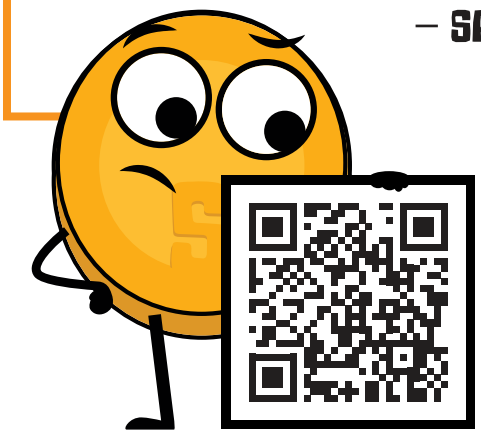
3.1 Actividad: ¡Subasta!

Actividad de Clase. Espera instrucciones del maestro para realizar esta actividad.

3.2 Inflación

Analizaremos el siguiente video sobre qué es la inflación. ¡Pon atención!

— SATOSHI



- Originalmente el término ***inflación*** se usaba para indicar:
  - La pérdida de valor de una moneda,
  - La devaluación de su poder adquisitivo provocada por el aumento de su oferta.

- Esta perdida de valor normalmente produce, en términos de dicha moneda:
  - Un aumento general y sostenido en el precio de todos los bienes y servicios.

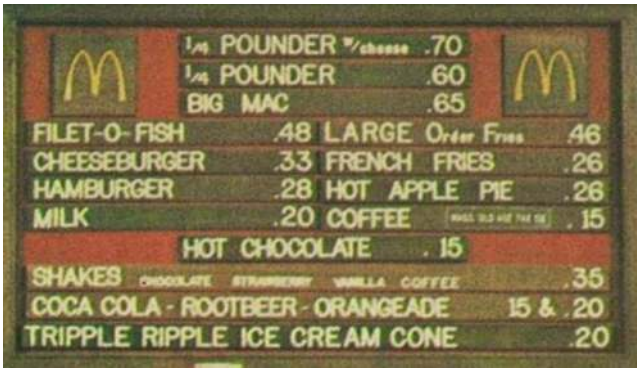
- El término "inflación" pasó a utilizarse también para indicar el aumento de precios.
  - Independientemente de la causa.

¿Porqué nos importa?

- Cuando más dinero persigue la misma cantidad de bienes:
  - Los precios suben.

- Si los precios de los productos aumentan más rápido que los sueldos y salarios:
  - Las personas se empobrecen.

McDonald's en 1970



McDonald's en 2020

¿Que nos enseñan los economistas modernos?

- Necesitamos estimular la inflación para poder administrar eficazmente a una nación.

- Si no incentivamos el gasto y la inversión (a través de la devaluación de la moneda):
  - Arriesgamos a una menor demanda.
  - Desatando una producción disminuida.
  - Llevando en el peor caso a una economía estancada.
  - Todo esto implica que es difícil, imposible o hasta no recommendable ahorrar.

Los Efectos del Dinero Fiat y la Centralización

- La situación actual nos incentiva a gastar. Es una teoría contraproducente.
  - No pensamos en un futuro más allá que un par de días, semanas o meses.
  - Deberíamos poder prepararnos para el futuro de nuestros nietos.
  - La inflación simplemente no nos permite tener disciplina financiera.

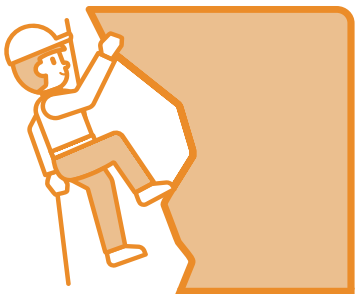
- Nuestras decisiones tienen consecuencias.
  - Esto se conoce como el "***costo de oportunidad***".

ESTUDIAR

- ☐ **Mejor opción de trabajo.**
- ☐ **Más preparado.**
- ☐ **Prestigio por el nivel académico.**

TRABAJAR

- ☐ **Sueldo percibido.**
- ☐ **Experiencia laboral.**
- ☐ **Prestigio social.**



➡ Uno tiene una *alta preferencia temporal* cuando prefiere las cosas que puede obtener ahora a las que podría obtener en un futuro.

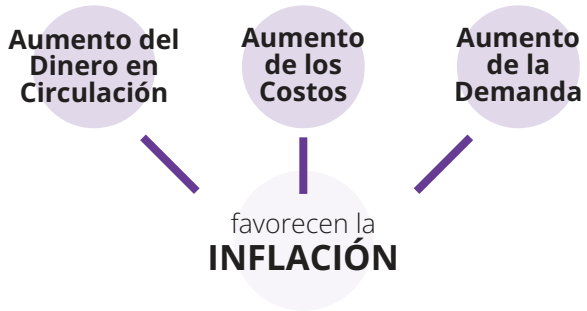
➡ Uno tiene una *baja preferencia temporal* cuando prefiere prescindir de cosas en el presente para obtener otras mejores en el futuro.

- La inflación fomenta una *preferencia temporal alta*, lo que significa que preferimos $100 hoy en vez de $200 en dos años.

- Nuestro objetivo debería ser crear una *preferencia temporal baja*.

Preferencia Temporal Alta	Preferencia Temporal Baja
Gastar Dinero	Ahorrar Dinero
Comida Rápida	Comida Casera
Ver Facebook	Leer un Libro
Ver Televisión	Hacer Ejercicio
Consumir Contenido	Creación de Contenido

Causas de la Inflación



En el siguiente video nos explican las tres razones por las que ocurre inflación.

1. Inflación de Costos o de Oferta

○ Aumenta el precio de los insumos, y es causada por:

• Regulaciones gubernamentales, guerras, sequías, dificultades en la cadena de suministro y otras situaciones.

• Alza en las tazas de impuestos incrementan el costo de las materias primas.

• Los trabajos especializados se vuelven más costosos.

- Falta de habilidades o recursos en una sociedad.

• Las nuevas tecnologías son muy caras.

- Con el tiempo disminuyen el costo de los productos.

2. Inflación de Demanda

○ La oferta de bienes no alcanza a cubrir la demanda.

○ Debido a una reducción de impuestos (o reducción en las tasas de intereses en los préstamos), se crea un aumento en el ingreso disponible.

• Empieza a circular en el mercado el exceso de dinero.

• Se compite por conseguir los mismos bienes con más dinero.

- Esto hace subir los precios.

○ Eventualmente aumenta la oferta, y luego los precios vuelven a bajar.

3. Inflación por Políticas Gubernamentales.

○ El gobierno financia el déficit con emisión.

• ¿Son auténticos los trabajos/proyectos que se crean a través de la inflación?

• ¿Por qué es importante para los gobiernos que la gente compre cosas con su dinero?

• ¿Que tipos de bienes compramos como sociedad cuando existe mas dinero en la economía? ¿Son bienes esenciales para vivir?

• ¿Qué sucede cuando las tasas de impuestos suben con más velocidad que el incremento en los salarios en una economía?

● La inflación significa que el trabajo que hiciste hace un tiempo tiene menor valor que el de hoy.

• El año pasado te pagaron $10; compraste diez almuerzos a $1 cada uno.

• Decidiste guardarlos.

- Y hoy hay más dinero en la economía circulando.

- Hay más gente que quiere comprar almuerzos.

- Pero la misma cantidad de almuerzos en venta.

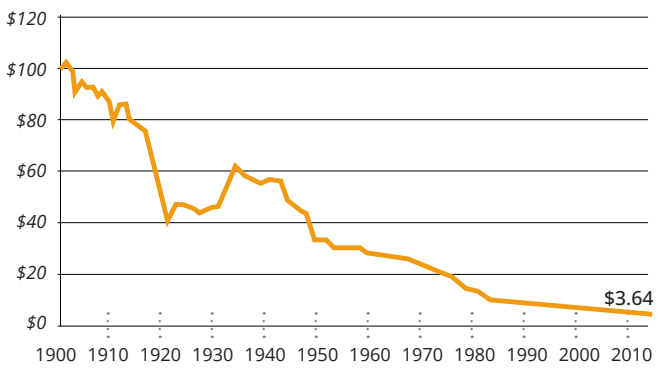
- El precio sube a $2 por almuerzo.

• Sólo podrás comprar cinco almuerzos con los $10 dólares que ahorraste.

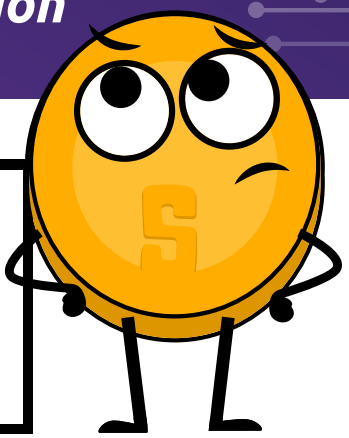
• En teoría, esto no tiene sentido. Si pones 8 horas de trabajo, esa realidad no cambia aunque hayan pasado 10 años. Esa energía debería poder quedarse contigo.

• Podríamos decir que la inflación es un tipo de robo de valor.

● En el siguiente gráfico podemos ver la perdida de valor del dólar (USD).



Los Efectos del Dinero Fiat y la Centralización

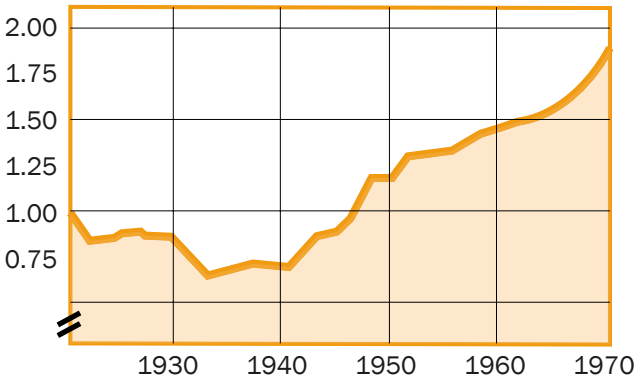


Inflación a través del Tiempo

- La inflación entre 1970 y 2020 fue mucho mayor que la del período de 50 años anterior, 1920 a 1970.
  - ¿Que pasará si seguimos en la misma trayectoria?
  - ¿Quien tuvo un castigo económico mayor, la generación de tus abuelos o la de tus padres?

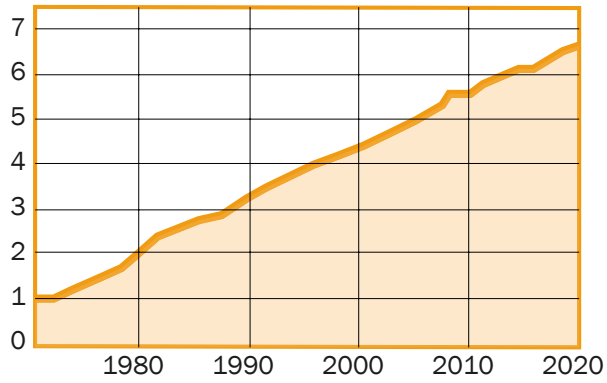
Para mayor visibilidad y análisis de otros periodos puedes ir aquí.

$1 de 1920 a 1970



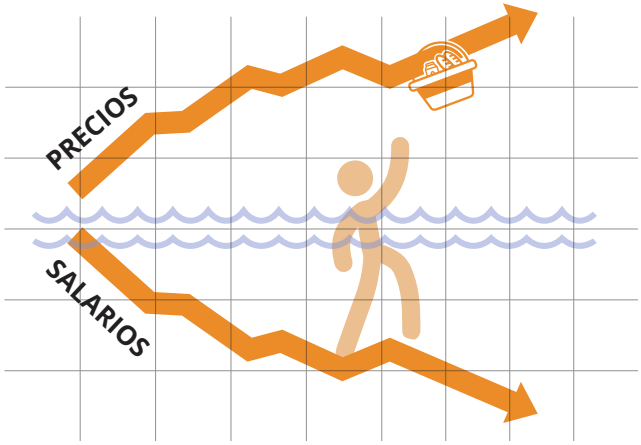
Resultado: **$1.94**
Tasa Promedio de Inflación: **1.33% por año**
Factor de Inflación Total: **93.72%**

$1 de 1970 a 2020



Resultado: **$6.67**
Tasa Promedio de Inflación: **3.87% por año**
Factor de Inflación Total: **566.60%**

- ¿Crees que los salarios subieron a la par de los precios?



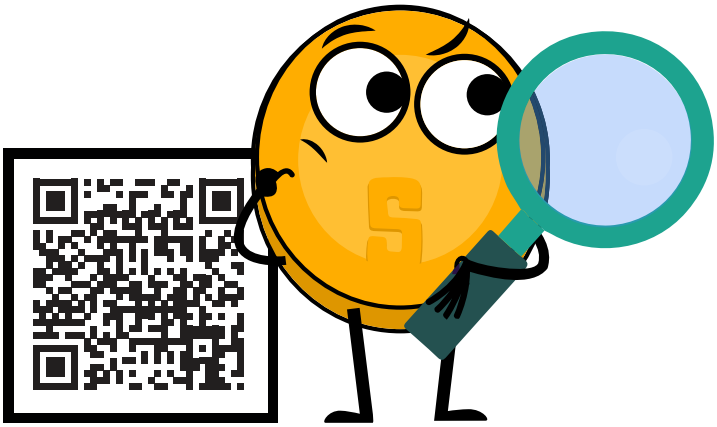
- Dicho desde otro punto de vista, lo que hoy (2022) compramos con $100, nos hubiera costado aproximadamente $7 en 1920.

- La inflación causa pérdida en el ***poder adquisitivo***:
  - Los aumentos en los salarios son menores que los aumentos en los precios de la comida.
  - Los individuos se ven obligados a reducir su consumo.
  - Se disminuye la capacidad de compra.

GANADORES DE LA INFLACIÓN	PERDEDORES DE LA INFLACIÓN
EL ESTADO Ya que con mayores precios y salarios aumentan sus ingresos por impuestos mientras que los gastos aumentan mucho menos.	**AHORRADORES** Que ven como sus ahorros cada vez valen menos.
LOS QUE PUDEN PRESTADO Ya que con la inflación les será más fácil recuperar el dinero, mientras que la deuda se mantiene fija.	**PRESTAMISTAS** Ya que cuando les devuelvan el dinero podrán comprar menos.
	PENSIONISTAS Y TRABAJADORES Ya que las pensiones y los salarios suelen subir menos que los precios.

3.3 Vigilancia

- Los gobiernos imponen regulaciones con el fin de encontrar y atrapar personas que lavan dinero o hacen otro tipo de transacciones ilegales.
    - La vigilancia es un arma de doble filo.
    - Cuanto más fraude ocurra, más vigilancia por parte del Estado y de compañías privadas:
        - Invaden nuestra privacidad gracias al progreso tecnológico.
        - Controlan nuestros movimientos en las redes sociales y económicas.
        - Intercambio de datos personales a cambio del disfrute de ciertos servicios.
- Algunas consecuencias son:
    - Estafas digitales, acoso en línea, extorsión, usurpación de identidad y otros problemas que ponen en peligro la privacidad y la seguridad de los usuarios.
    - Nuestras compras con tarjetas se registran, analizan y se vigilan.
        - A menos que compremos bienes y servicios en efectivo.
    - Si alguien consigue tu contraseña de tu banca en internet, o hackea los servidores centralizados, tendría acceso a toda la información.



Necesitamos un dinero que resguarde nuestra privacidad y no comparta toda nuestra información personal con gobiernos y empresas privadas.

3.4 Restricción

- Es que es difícil y costoso mover dinero entre naciones.
- Los gobiernos controlan los intercambios de divisas, aunque se haga entre dos personas conocidas.

Aquí hay una lista de políticas y formas en que esto puede suceder:

Los Efectos del Dinero Fiat y la Centralización

Políticas Gubernamentales

- *Control de Capitales*: Se restringe la cantidad de dinero que sus ciudadanos pueden transferir, cambiar o llevar al extranjero.
    - Ejemplos:

- Ar*gentina, Rusia, Indonesia, Cuba y China.*
- *El ciudadano promedio de China, solo puede convertir hasta $ 50.000 de renminbi (aprox. $8.000 USD) cada año.*

"La única solución que hemos encontrado en Cuba es Bitcoin. Estamos ahora mismo en las mismas igualdades, la misma posibilidad de competir con cualquier otro país, porque tenemos acceso pleno, libre, sin sanciones ni prohibiciones a esa tecnología que nos permite crear, crecer y conectar."

-Eric García Cruz, emprendedor cubano y entusiasta de Bitcoin.

Políticas Bancarias

- Los bancos tienen límites sobre la cantidad de efectivo que se puede retirar de una cuenta, o tienen un máximo que se puede transferir.

- La mayoría de estas transacciones tienen comisiones.
    - Ejemplos:

- *Grecia, tras la crisis de 2015, sus ciudadanos solo podían retirar $60 euros al día,*
    - Este es un claro recordatorio de quién realmente controlaW tu dinero.
- *En El Salvador, la remesas representan el 23% de su producto interno bruto (PIB).*
    - En el 2020 fueron casi $6 mil millones de dólares. Alrededor del 60% proviene de empresas de remesas y el 38% de instituciones bancarias.
    - Empresas como Western Union tienen tarifas elevadas.
    - Especialmente para montos inferiores a $1,000 USD.

Comisiones o Cargos

- Estos cobros solo enriquecen a las instituciones bancarias.

- Además, incrementan la brecha entre ricos y pobres.
    - Para montos pequeños, como de diez dólares, las comisiones pueden llegar a ser hasta de más de tres dólares, o el 33%.
    - Para 100 dólares, las tarifas oscilan entre el 12% y el 15%.

Horario

- Para enviar/recibir una remesa:
    - Tanto el remitente como el destinatario deben acudir a la sucursal más cercana.
    - Esto debe ser durante horario laboral, por supuesto.

Seguridad

- Acudir a las oficinas de Western Union representa riesgos adicionales:
    - Las personas deben llevar su dinero en efectivo, aumentando las posibilidades de ser robados.
    - Si los servidores centralizados fallan (lo que pasa frecuentemente), se podrían negar el acceso a los fondos de cualquier cliente.

3.5 Centralización vs. Decentralización

- La centralización de las economías modernas produce:

• Censura, abuso de poder, corrupción, desigualdad de oportunidades, desigualdad de riqueza, y fuentes únicas de fallos.

- Los bancos operan por medio de servidores centralizados.

• Tienen acceso todas las actividades financieras de sus usuarios.

¿Qué saben los bancos de sus clientes?

- Cuánto te pagan.
- En qué gastas tu dinero.
- A quién le mandas dinero.
- Todo lo relacionado con tu cuenta.

Características de un Sistema Centralizado

- Tienes que confiar que la organización centralizada mantendrá tus datos seguros.
- Tienen completo control del sistema y de tus datos.

- Si los servidores principales se ven comprometidos, tus datos están en riesgo.

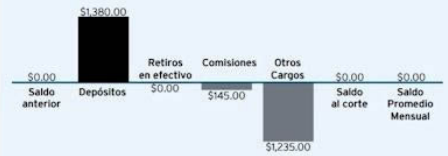
Las divisas digitales de los bancos centrales son la continuación del sistema actual pero de forma digital. Es decir: mutables, censurables, cerradas, centralizadas, exclusivas, y vigilantes.

Carlos Pérez Pérez.
Av. Independencia # 543 interior 2.
Col central C.P 34004

BANCO

Contrato: 25687451
Sucursal 1
Cuenta: 123321
Clave Interbancaria: 00000123321
Cliente: 963258
RFC: PEPC920212R47

Comportamiento

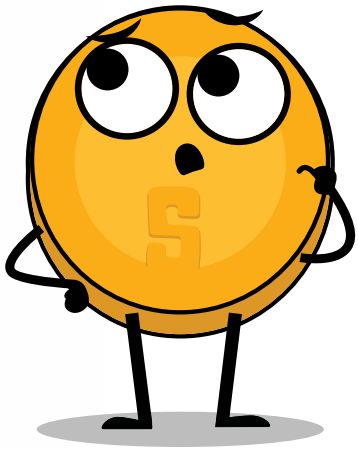


Resumen En Pesos Moneda Nacional

Saldo anterior	0.00
Depósitos	1,380.00
Retiros en efectivo	0.00
Otros cargos	1,235.00
Saldo al corte	0.00
Saldo promedio mensual	0.00

Detalle de Operaciones En pesos Moneda Nacional

FECHA	CONCEPTO	RETIROS	DEPÓSITOS	SALDO
25 DIC	SALDO ANTERIOR			0.00
11 ENE	PAGO RECIBIDO DE BBVA BANCOMER			
	POR ORDEN DE MAURICIO DEL			
	MORAL DURAN REF.0000001			
	ARTICULOS RASTREO:			
	BNET01001601110002067854		1,380.00	1,380.00
11 ENE	IVA POR COMISION MANEJO DE			
	CUENTA	23.20		1,356.80
11 ENE	COMISION PENDIENTE MANEJO DE			
	CUENTA B110401166	145.00		1,211.80
11 ENE	COBRO DE 600501077330			
	MAS910614BR6 Domi Asistencia			
	Familiar 10	89.00		1,122.80
11 ENE	RETIRO POR TRASPASO	1,122.80		0.00
22 ENE	COMISION MANEJO DE CUENTA			
	PENDIENTE POR: 145.00 MAS			
	I.V.A.			0.00



Los Efectos del Dinero Fiat y la Centralización

¿Cómo contrarrestamos estos fenómenos, causados por malas políticas gubernamentales?

Características de un Sistema Descentralizado

Se describe cómo un sistema de *igual a igual* o de *P2P* porque:

- Las personas no tienen que identificarse para interactuar y estar interconectados entre sí a través de internet.
- Cada quien es responsable de su propio dispositivo pero presta y comparte sus recursos.
- Si hay un ataque a la red, los hackers tendrían que tener control de la mayoría de computadores — esto es casi imposible.
- En caso de que hubiera un error en un servidor, el resto no se vería afectado.
- Logra una sociedad más justa- quita el control a las corporaciones poderosas.

3.6 Conclusión

Preguntémonos de nuevo, ¿habrá solución a los problemas del dinero actual?

ESTO **ERA DINERO**

=

Respaldado por oro y plata.

ESTO **ES PAPEL**

=

Respaldado por "la buena fe y el cédito del gobierno".

ESTO ES EL FUTURO

Respaldado por los ciudadanos del mundo con el uso de la tecnología.

=

Clase #4

Bitcoin

4.1 ¿Por qué se creó Bitcoin?
- ¿Los problemas a solucionar?
- ¿Cómo se solucionaron estos problemas?
- ¿Quién los solucionó?
- ¿Cuáles dificultades enfrentó Satoshi?
- ¿Cuál era el dilema de los Generales?
- ¿Qué tiene que ver esto con Bitcoin?

4.2 Introducción al Bitcoin
4.3 Diferencias entre Bitcoin y Fiat
4.4 Los Participantes de Bitcoin

4.1 ¿Por qué se creó Bitcoin?

El ataque en el 2001 a las Torres Gemelas de Nueva York fue un golpe durísimo para la economía mundial. Como consecuencia, con el apoyo del sector privado y el objetivo de facilitarle financiamiento hipotecario a las personas de ingresos más bajos, E.E.U.U. comenzó a bajar las tasas de interés rápidamente a niveles nunca antes vistos.

De tal forma, se les dió créditos a personas sin ingresos, activos, ni empleo. Este tipo de hipotecas fue bautizada como "hipotecas subprime", y por supuesto, tenían alta probabilidad de impago. Los efectos de la crisis se viven hasta hoy. Su estallido se dió el 15 de septiembre del 2008, cuando el banco de inversión Lehman Brothers se declaró en bancarrota. A partir de ese momento, Estados Unidos sufrió un colapso económico y luego le siguió el resto de los países desarrollados. En consecuencia, día a día creció la desconfianza en los bancos por la toma de riesgos excesivos y la poca regulación en la industria.

¿Los problemas a solucionar?

- La falta de soberanía individual.
- La centralización de los bancos.
- La inflación.
- La vigilancia.
- La necesidad de intermediarios.
- La poca accesibilidad a los servicios bancarios.
- Los altos costes de las remesas internacionales.
- Entre otros.

¿Cómo se solucionaron estos problemas?

- Con el uso de una tecnología desarrollada en 1991, *blockchain*.

El *Blockchain* (o Cadena de Bloques) es la tecnología detrás del **Bitcoin**, la famosa moneda digita. El Blockchain es una base de datos compartida online que funciona como un libro de registro de transacciones. Es una red de pago descentralizada *peer-to-peer*. Utiliza claves criptográficas y está distribuida y compartida en muchos ordenadores, por lo que reduce el riesgo de fraude y falsificación.

¿Quién los solucionó?

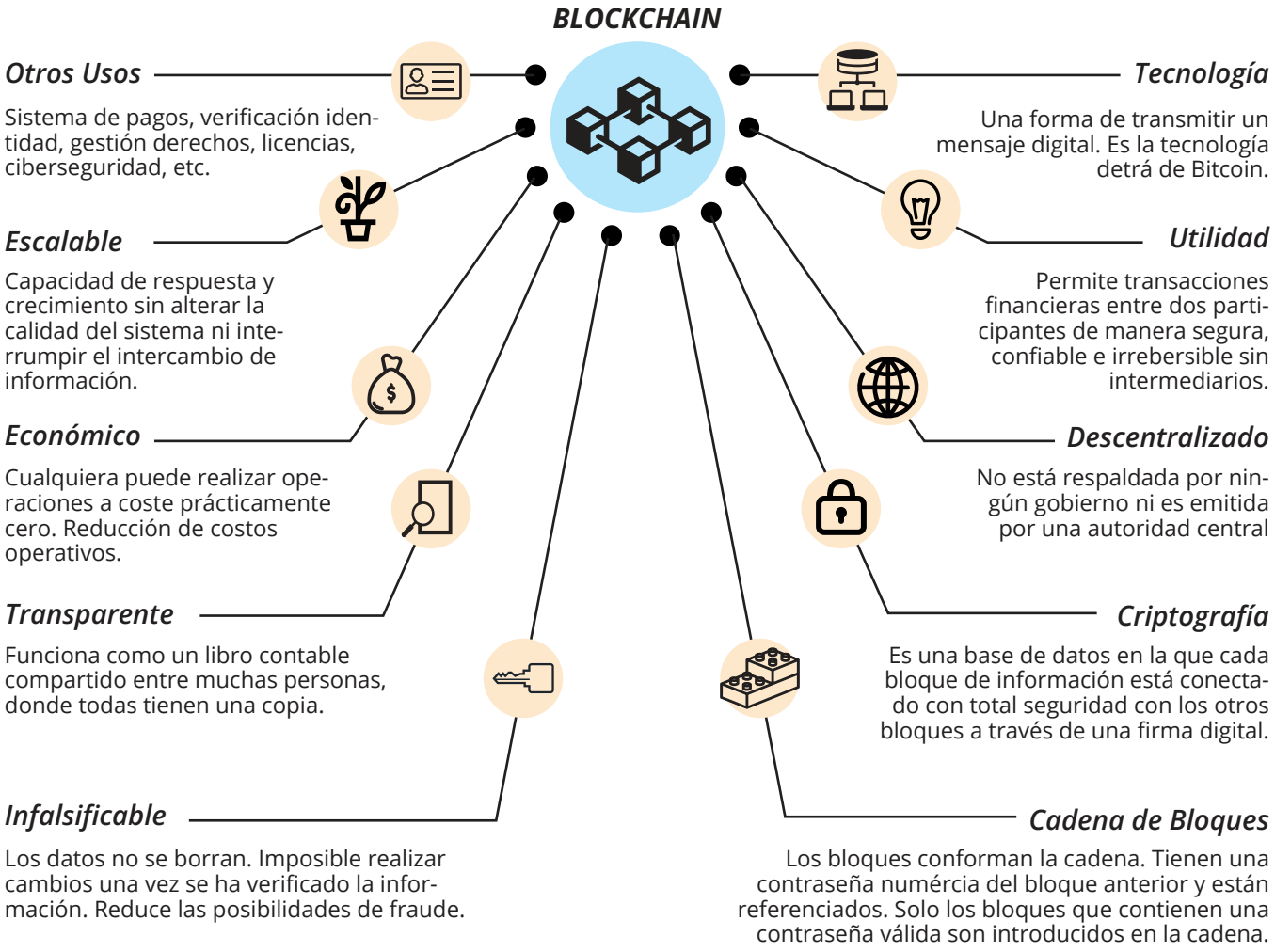
- *Satoshi Nakamoto* apareció en octubre del 2008 y su identidad todavía es un completo misterio.

- Propuso su idea de un nuevo sistema de efectivo electrónico. Este dinero se llamaría ***bitcoin***.

- Dedicó su tiempo a crear una guía para explicar un nuevo medio de pago que:
  - Posibilita la ejecución de transferencias de valor rápidas, y a bajo costo.
  - No puede ser controlado ni manipulado por gobiernos o entidades financieras.

- Gracias a esta persona, o grupo de personas (no se sabe), existe una solución al problema del *"doble gasto"*.
  - Ahora es imposible que alguien gaste el mismo dinero virtual en dos sitios diferentes.

- Su documento de nueve páginas conocido como un *Whitepaper* (Papel Blanco).



• Lo compartió a una lista de correos electrónicos con los *Cypherpunk*:

- Un grupo muy activo con discusiones técnicas.
- Abarcaban matemáticas, criptografía, ciencias de la computación, discusiones políticas y filosóficas e incluso argumentos personales.

● Satoshi tenía cinismo hacia el sistema monetario y bancario tradicional.

• Esto se puede ver en el *bloque génesis*, donde publicó un mensaje que decía:

Aquí puedes descargar el Whitepaper de Satoshi Nakamoto.

Bitcoin

"The Times 03/ene/2009 Canciller al borde del segundo rescate para los bancos."

- Satoshi Nakamoto, Genesis Block.

- Hace referencia a un artículo del periódico *Times* titulado "*Canciller al borde del segundo rescate de los bancos*".
  - El canciller británico debía decidir si inyectar billones de Libras Esterlinas más en la economía con el fin de rescatar a los bancos.

- Estos son otros datos básicos que sabemos sobre Satoshi, su *Whitepaper* y la creación de **Bitcoin**:

1. **Solo tiene 9 páginas.**

2. **Busca un Sistema de "dinero electrónico" sin intermediarios.**

3. **La palabra blockchain no aparece en el libro.**

4. **Define una moneda digital como una cadena de firmas.**

5. **El término minería surge de una comparación didáctica.**

6. **No persigue transacciones más veloces, si no más seguras.**

7. **El aumento del tamaño de la cadena se calculó en 4,2 MB/año.**

- La primera transacción de ***bitcoins*** fue de Nakamoto a Hal Finney.

- La última "señal de vida" de Satoshi fue con Gavin Andersen, un desarrollador de software:
  - *"...paso a otras cosas,...en buenas manos con Gavin y todos."*

- En mensajes públicos, e incluso en mensajes privados que luego se publicaron, Nakamoto nunca habló de nada personal. Todo se trataba de bitcoin y su *código*.

- Muchas personas afirmaron ser Satoshi. Aún no sabemos quién es.

- Se estima que Satoshi tiene aproximadamente 980,000 bitcoin.

¿Cuales dificultades enfrentó Satoshi?

- ¿Podría alguien mandarle el mismo dinero a dos personas simultáneamente?

- En internet ¿quién puede confiar en quien está del otro lado?

- ¿Cómo sabemos si alguien tiene suficiente dinero en su cuenta (o en su monedero) para comprarle un producto a otro?

- ¿Cómo se asegura de que una red descentralizada pueda tomar decisiones correctas, incluso si algunos de los *nodos* (participantes conectados) en ella se vuelven deshonestos?

- ¿Podemos crear un sistema distribuido y confiable que no asuma automáticamente que los participantes van a actuar éticamente y trabajarán en interés del grupo?

- ¿Cómo sabemos que la persona que quiere recibir dinero a través de este sistema es quien dice ser?

"Problema del Doble Gasto" = "Problema de los Generales Bizantinos"

¿Cuál era el dilema de los Generales?

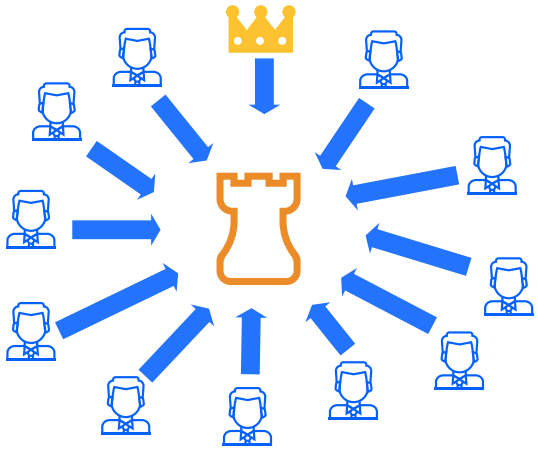
- El problema de los Generales Bizantinos es una metáfora que narra la dificultad de transmitir información fiable sin la intervención de un coordinador central de confianza.

¿Cuál es la alegoría?

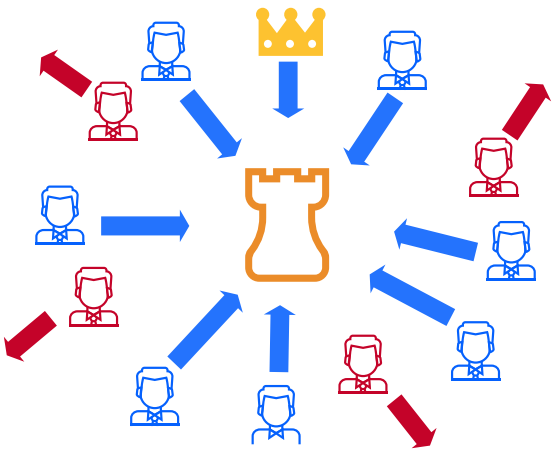
- Hay un castillo en Persia, que está muy bien abastecido y fortificado.
- Los generales bizantinos han rodeado el castillo y planean lanzar un ataque.
- Dado que el ejército está tan disperso, no existe un control centralizado.
- Los generales se comunican entre ellos por medio de mensajeros.
- Las dos posibles órdenes son "atacar" y "retirarse".
- Deben ponerse de acuerdo para atacar al ejército persia, y hacerlo simultáneamente.
- Si cualquiera de ellos lo intentara por separado, perderán la batalla.
- Si existe un traidor, podría conseguir que los leales no se pongan de acuerdo.
    - Por ejemplo, le podría decir a un general que ataque y al otro que se retire.
- Una mañana, un general recibe el siguiente mensaje: "*El ataque se producirá el martes*". No lleva la firma de ninguna autoridad central.

¿Cómo puede el general tener la certeza de que se trata de una orden verdadera y no de un engaño del enemigo transmitiendo información contraria a la estrategia del ejército?

¿Que sucede si quien mandó el mensaje es traidor y planea traicionar al ejército? ¿Qué pasa si el mismo general es corrupto y busca sembrar la discordia entre los otros generales?



Los ataques coordinados conducen a la victoria.



Los ataques descoordinados conducen a la derrota.

La solución a este problema se usó originalmente como método para evitar el spam por email.

¿Que tiene que ver esto con Bitcoin?

El problema de los generales bizantinos describe lo siguiente:

- La dificultad que tienen los sistemas descentralizados para ponerse de acuerdo sobre una sola verdad.

- Es el mismo que se tiene cuando se realiza una transferencia de dinero sin un intermediario confiable.
  - Se requiere de una manera de verificar que el mensaje no ha sido modificado, lo cual no se había logrado hasta la aparición de **Bitcoin** con su mecanismo de *consenso*.

- El uso de la criptografía es esencial en este proceso, pero ¿qué es *criptografía*?
  - El arte de crear *mensajes codificados con claves secretas* con el objetivo de que no pueda ser descifrado salvo por la persona a quien está dirigido o que tenga la clave.

- **Bitcoin** también utiliza un mecanismo de *prueba de trabajo* y una *cadena de bloques* para resolver el problema del "*doble gasto*".

- **Bitcoin** logra:
  - 1) Transferir un activo digital (o dinero) a otro usuario a través de Internet.
  - 2) De manera que solo el propietario pueda iniciar la operación.
  - 3) Únicamente el destinatario pueda recibirlo.
  - 4) Todo el mundo pueda validar la transferencia.
  - 5) Y esta sea reconocida por todos los participantes.
  - 6) Al igual que ser inmutable, o imposible de revertir o borrar.
  - 7) Todo ello realizado de manera totalmente *distribuida* y *descentralizada.*

- En el marco de las cadenas de bloques, cada General es un *nodo en la red*.

- Los nodos deben llegar a un convenio para determinar el estado actual del registro de contabilidad compartido.
  - Si la mayoría de la *red* en la *blockchain* está de acuerdo, modifican los balances de cuentas por pagar y por cobrar de los usuarios.
  - Si una gran mayoría de la red es maliciosa, el sistema es vulnerable a fallas.

4.2 Introducción al Bitcoin

*¿Qué es **Bitcoin**? ¿Qué es **bitcoin**?*

- Es muchas cosas:

- **Dinero**. Es una moneda virtual e intangible que cumple las tres funciones del dinero tradicional: una unidad de cuenta, un depósito de valor y un medio de intercambio.

- **Software**. Es software que puede descargar y ejecutar en cualquier computador.
  - Un *sistema de pago* sin un banco central o una autoridad única.

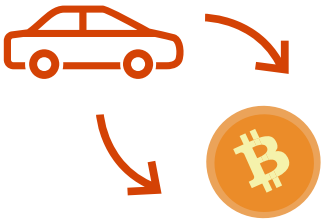
- **Red**. Es un conjunto de personas y computadores trabajando a través del consenso para funcionar sin falla.

Es una moneda, tal como otras.

Pero es digital.

Sin control de una autoridad central.

Es intercambiable por bienes o servicios.



Es portable y segura.

Puede ser usada en miles de comercios y tiene el mismo valor en todo el mundo.

*¿Cuál es la diferencia entre **Bitcoin** y **bitcoin**?*

Bitcoin con '**B**' mayúscula se refiere a la *red* de computadores que trabaja con el mismo programa, mientras ***bitcoin*** con '**b**' minúscula se refiere a el activo digital ($) que se maneja dentro de la red. Dicho de otra forma, ***bitcoin*** es una unidad de la moneda virtual cifrada mediante criptografía, que nos sirve para intercambiar valor dentro de la red **Bitcoin**.

¿Cual es su función principal?

- Permite la transferencia de pagos persona a persona (*P2P*), sin intermediarios, de forma económica, y sin barreras internacionales. Almacena valor.

¿Qué avance tecnológico ha logrado? ¿Porqué revolucionará la banca?

- Impide que la gente pueda gastar el mismo dinero dos veces.
- Elimina la necesidad de una autoridad central para supervisar las transacciones.

¿Qué lo hace valioso?

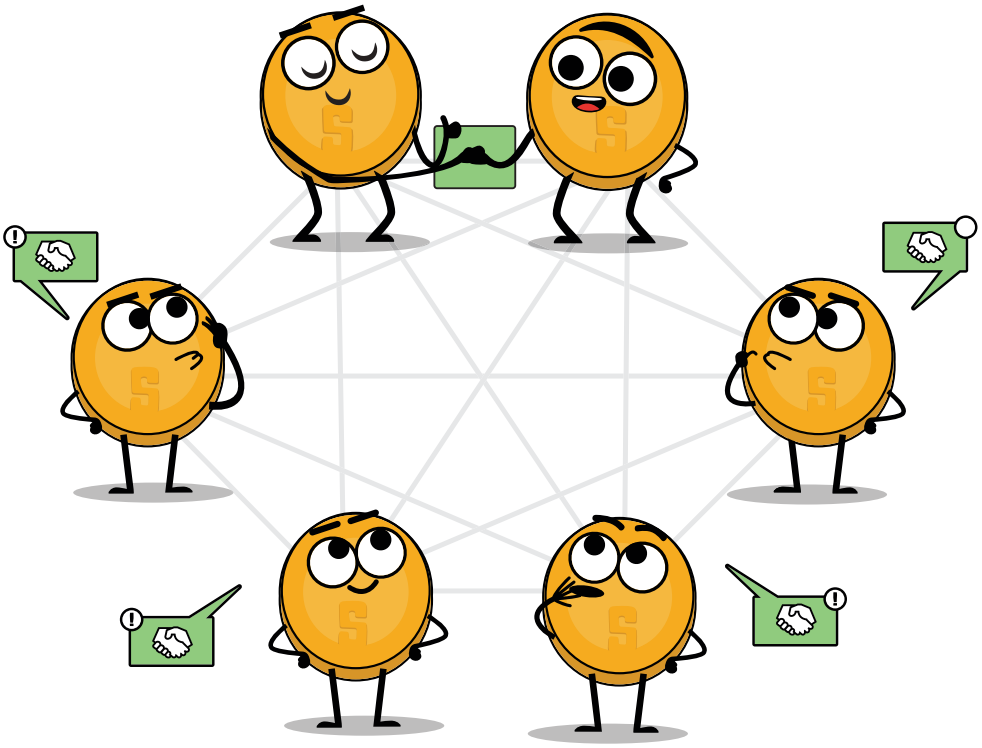
Bitcoin

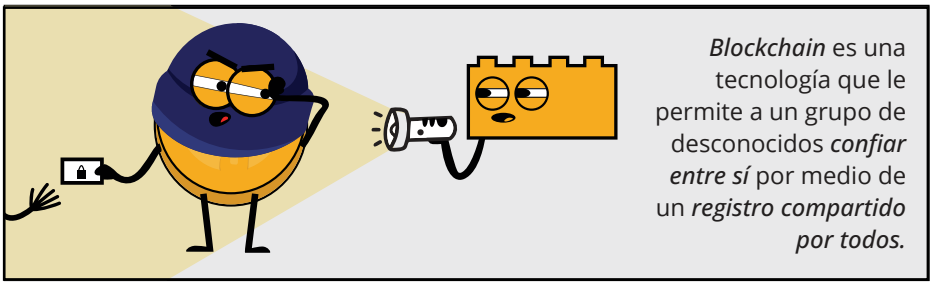
*¿Cuál es la relación entre la cadena de bloques y **Bitcoin**?*

- La cadena de bloques es el libro público donde se registran de forma permanente las transacciones más importantes de **Bitcoin**.
- **Bitcoin** es la única cadena de bloques que registra transacciones realizadas con la moneda ***bitcoin***.

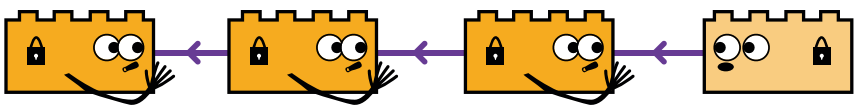
*¿De qué están hechos los **bitcoin**?*

- De nada que se pueda tocar físicamente, como un billete.
- Son sólo cadenas de números y letras digitales.
- Una identidad única (tal cómo tu huella digital te da tu identidad).





Blockchain es una tecnología que le permite a un grupo de desconocidos *confiar entre sí* por medio de un *registro compartido por todos.*



Blockchain es un registro de transacciones seguro porque está distribuido entre los integrantes de una red.

Cada transacción queda grabada permanentemente para todos y de esta forma ningún movimiento puede ser oculto.

Los datos se almacenan en bloques encriptados (*blocks*) que se conectan de manera secuencial con cadenas (*chains*), y hacen difícil modificar la información sin el consenso de toda la red.

Sus características lo hacen una tecnología que podría volver más trasparentes procesos como el gasto público de los gobiernos e incluso elecciones.

*¿**Bitcoin** es anónimo?*

- No, es *seudónimo*. Las transacciones son visibles, accesibles y transparentes para todos.

- Las personas se identifican no con nombre y apellido sino con cadenas de cadenas de letras y números.

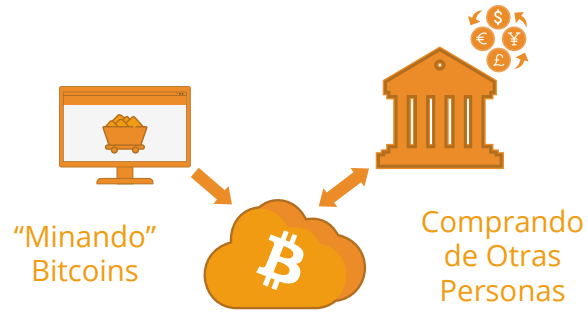
*¿Quién puede usar **Bitcoin**?*

- A diferencia del sistema bancario tradicional, cualquier persona que tenga acceso al internet.

*¿Cómo puedo conseguir **bitcoin**?*

- Se *compra* en línea a través de plataformas de intercambio o *exchanges*.

- Se *crean nuevos* bitcoin a través de un proceso de trabajo llamado *minería*.



*¿Cuales son las barreras de entrada a **Bitcoin**?*

- Se necesita acceso a internet para poder hacer transacciones con BTC.

- Algunos países prohiben las entradas pero es imposible prohibir el intercambio.

*¿En donde se almacenan los **bitcoin**?*

- En un monedero con acceso a nuestras claves privadas o en un exchange.

¿Cómo puede tener valor una moneda que no existe en el mundo físico y que no está respaldada por nada, ni por nadie?

- El valor crece con *confianza*, *escasez*, *utilidad*, *nivel de demanda*, entre otros factores.

*¿Es seguro el **Bitcoin**?*

- El objetivo de la minería es desincentivar a los malos actores y dificultar comportamientos indeseados como el doble gasto o el spam.

- La criptografía protege la información de una manera muy segura. Se usan:
  - **Claves públicas** (similar al número de una cuenta bancaria pero único en cada transacción).
  - **Claves privadas** (similar a un PIN secreto perteneciente a dicha cuenta bancaria).

¿Quien y cómo se asegura de que las transacciones se ejecuten sin fallas?

- A través de la los mineros y la minería.

- El objetivo es desincentivar a los malos actores y dificultar comportamientos indeseados.

*¿Cuales son algunas de las ventajas de **bitcoin** frente al fiat?*

- El precio del bitcoin es el mismo en todos los países del mundo.

- No existen fronteras.

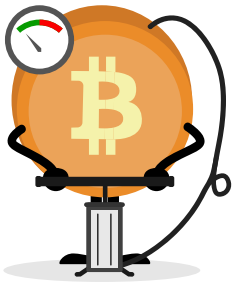
- Su inflación es controlada y su emisión predefinida.

- Los gobiernos no tienen poder de decisión sobre su gobernanza.

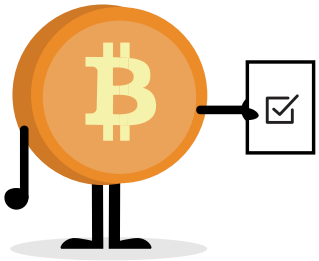
4.3 Diferencias entre Bitcoin y Fiat

	Bitcoin	Fiat
Tangibilidad	Es una moneda virtual y sólo puede ser usada en forma digital.	Puede ser utilizada tanto en forma física (monedas y billetes) como digital (i.e. cheques, apps).
Regulación	Se crea a través de la minería y se controla por medio de un sistema distribuido y descentralizado de computadores.	La crea y controla un gobierno central y/o banco central. Según esto, es la moneda de curso legal en el país cuyo gobierno autoriza su creación.
Gobernanza	Un mecanismo de consenso voluntario y requiere altos niveles de acuerdo.	Gobernada por el gobierno central.
Valor	Respaldado por la confianza de los usuarios. Entre más usuarios , más estable se convertirá.	Determinado por la oferta y demanda y vulnerable a la inflación.
Oferta	Limitado a 21 millones.	No tiene límite.
Validación de Transacciones	A través de la criptografía y uso de tecnología blockchain.	A través de un banco o intermediario.
Costos de Transacción	Mínimos.	Significativos, ya que existen intermediarios.
Tiempo y Rapidez de la Transacción	Diez minutos, en promedio (en Bitcoin), e instantánea (en Lightning Network).	Instantánea (en efectivo), días o hasta meses (transacciones bancarias).
Seguridad	Criptografía (rama de las matemáticas). Previene un ataque del 51% de los nodos.	Seguridad interna de bancos, y puede ser afectada negativamente por las fluctuaciones en las pólizas gubernamentales.
Cambios	Las transacciones de bitcoin no se pueden revertir, cambiar o cancelar.	Es común que haya disputas en las transacciones, y cambios o reversiones.

Bitcoin vs. Fiat

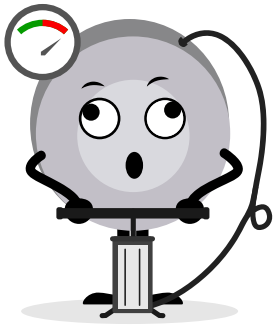


Inflación controlada, cantidad en circulación predecible y predefinida.

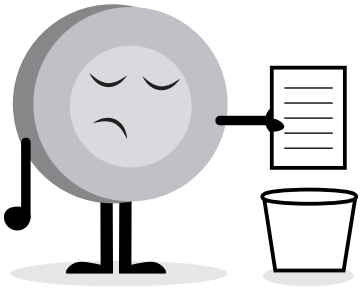


Sólo se pueden aplicar cambios si los usuarios los aceptan.

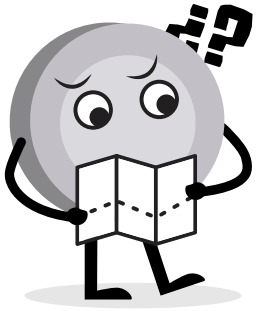
No tienen fronteras, puede ser aceptada por cualquier persona en el mundo.



Inflación a niveles récord y puede ser devaluada al imprimir tantos billetes como quiera.



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.

Ejercicio Práctico. Termina de completar el ejercicio de la Clase#1, en la página 16. En la columna de 'Bitcoin', marca con una **X** si el artículo cumple con la característica indicada. ***¿Cuál artículo escogerías como dinero?***

4.4 Los Participantes de Bitcoin

Para entender cómo participa alguien o un sistema en la red **Bitcoin**, nos debemos preguntar lo siguiente:

- *¿Dicha persona o computador puede ver solo las transacciones en las que participa?*
- *¿Tiene acceso a más información?*
- *¿Cuáles son las transacciones que puede realizar?*
- *¿Cuáles son los permisos tiene sobre la red?*
- *¿Cómo interactúa con la red?*
- *¿Tiene acceso a una copia de toda la cadena?*

En la gráfica de abajo podemos ver los diferentes participantes en la red de Bitcoin.

- **1. Mineros**. Equipos de computación especializados:
  - Compiten en resolver rompecabezas matemáticos entre sí, para crear nuevos ***bitcoins***.
  - Confirman transacciones y mantienen la seguridad de la red.
    - Igual que a los empleados en un banco; se les paga por su trabajo realizado.

- **2. Exchanges o Intercambios.** Intercambian monedas fiat por ***bitcoin*** y otros tipos de *criptomonedas*.
  - Ofrecen una manera de entrar y salir del mercado para aquellos que no son mineros.
  - Similar a los bancos; ofrecen servicios a los usuarios.

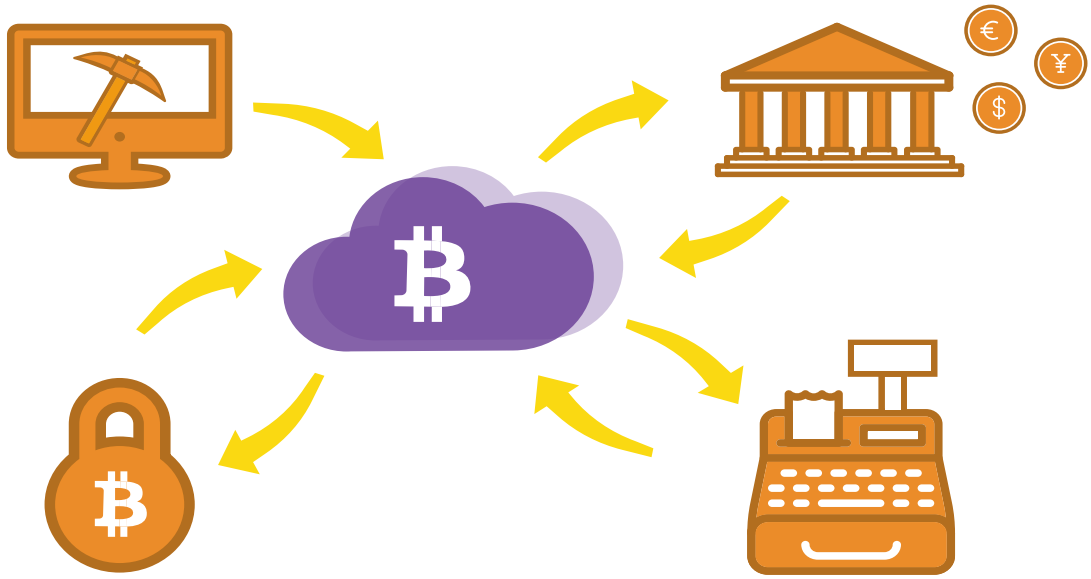
- **3. Monederos**. Aplicaciones usadas para almacenar, mandar y recibir ***bitcoin***.
  - Esto es similar a las cuentas bancarias o las apps para transferir dinero por internet.

- **4. Nodos.** Dispositivos conectados a una red digital que validan, transmiten, procesan y almacenan transacciones BTC. (Además de ser monederos, tienen muchas otras funciones).
  - Constan de dos cosas: hardware y software.
    - Similar a un móvil y un app.
    - El hardware es el material físico necesario para ejecutar el software.

- **5. Desarrolladores.** Mantienen y proponen mejoras al código.

Los **mineros** crean ***bitcoins*** usando computadoras para resolver funciones matemáticas, el mismo proceso también verifica transacciones anteriores.

Los **Intercambios** harán las conversiones entre monedas convencionales y ***bitcoin***, ofreciendo una forma de ingresar al mercado para los no mineros, así como una forma de retirar dinero.



Los usuarios descargan un **monedero** que funciona como una dirección de correo electrónico, proporcionando una forma de almacenar y recibir moneda. Los ***bitcoins*** se pueden transferir de un monedero a otro usando un navegador web o una aplicación de teléfono inteligente.

Las empresas crean un **monedero** de la misma manera que un usuario individual, generalmente usando un botón de sitio web para habilitar un pago en ***bitcoin***. Para empresas con establecimiento físico, los códigos QR se pueden usar para permitir que los clientes paguen rápida y fácilmente.

Clase #5

Compra, Custodia y Movimiento de Bitcoin

5.1 Rampas de Entrada y Salida
- ¿Tengo suficiente dinero para comprar bitcoin?

5.2 Custodia de Bitcoin
- Tipos de Monedero y Lightning
- ¿Como envío o recibo satoshis?

5.3 El Ciclo de una Transacción (on-chain)
- ¿Qué es una transacción de Bitcoin?
- Puentes y Paradas para realizar Transacciones
- ¿Cómo funciona una transacción paso a paso?
- UTXO - “Monedas no Gastadas”
- La Confirmación de una Transacción

Compra, Custodia y Movimiento de Bitcoin

5.1 Rampas de Entrada y Salida

- El primer paso para obtener ***bitcoin*** es comprarlo. Existen diversas alternativas:
  - *Casas de intercambio, brokers, cajeros BTM's, compañías fintech, tarjetas de regalo, etc*.

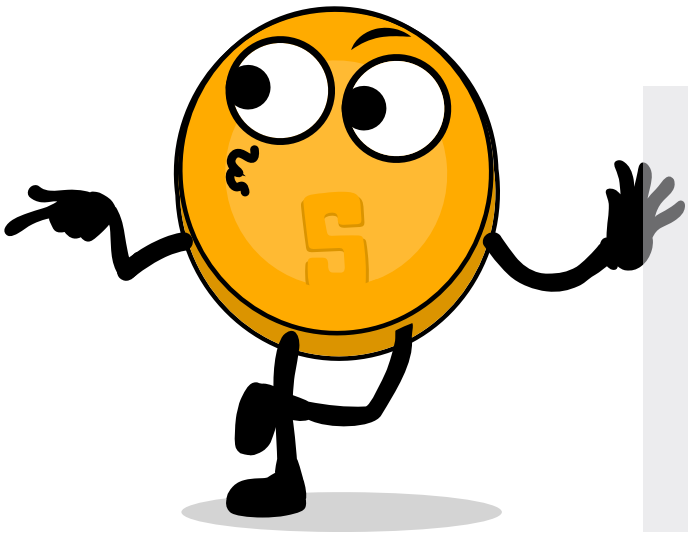
- Se intercambia dinero convencional (*euros, dólares, etc.*) por su equivalente en ***bitcoin***.

- Los servicios que proporcionan estas funciones son "***rampas de acceso***".

- Los gobiernos pueden regular las rampas de entrada y salida.
  - Podrían prohibir que los bancos envíen dinero hacia o desde un intercambio de ***bitcoins***.
    - Lo cual afectaría nuestra capacidad de comprar y vender ***bitcoins*** pero, sería imposible *impedir enviar/recibir* ***bitcoin***.

¿Tengo suficiente dinero para comprar bitcoin?

- **BTC** es la unidad común de la moneda ***bitcoin***.



- Puede utilizarse el símbolo ₿ para referirnos a ***bitcoin***, al igual que se utiliza (**USD**) o **$** para el dólar estadounidense.

- ***Bitcoin*** tiene un valor equivalente a todas las divisas del mundo en cualquier momento.
  - Por ejemplo, en este instante:

  1 ₿ = US$21,464 y 1₿ = $95,288,229 COP (Pesos Colombianos)

- ***Bitcoin*** es mucho más divisible que $1USD, $1USD = 100 centavos. No existe 1/2 centavo o 1/10 de centavo.

- Un ***Satoshi*** (o ***Sat*** para abreviar), es la denominación más baja en la moneda ***bitcoin***.
  - 1 BTC = 100,000,000 sats ≈ 0.0003 USD
  - Esto quiere decir que un ***bitcoin*** se puede dividir en cien millones de unidades.

- ***Sesgo de Unidad:*** Falsa creencia...
  - No se tiene que comprar 1 ***bitcoin*** entero, se pueden comprar los ***Sats*** que se quieran.

'Si lo añades poco a lo poco y lo haces así con frecuencia, pronto llegará a ser mucho."

- Hesíodo

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

5.2 Custodia de Bitcoin

*¿Cómo se **custodia** **bitcoin**?*

- Cuando se compran ***Sats*** en un sitio web, lo más probable es que los acrediten a un "monedero" *(o una billetera)* virtual.
  - Similar a recibir un crédito en una cuenta bancaria cuando se transfiere dinero a ella.

- Puede parecer que la persona es dueña de su ***bitcoin***, pero en realidad, el dinero está en posesión de un tercero.

- Por lo tanto, es importante entender los riesgos de invertir en ***bitcoin*** y comenzar por:
  - Conocer las mejores formas de custodiar ***bitcoin*** en el mercado.
  - Descubrir lo que es un *monedero*.
    - *Cual ofrece la mejor seguridad.*
    - *Cómo escoger el más adecuado para los requisitos de cada quién.*
  - Analizar las ventajas y desventajas de los monederos que seleccionemos.
    - *Comprender que no existe un monedero ideal que satisfaga todas las necesidades.*

Tipos de Monederos y Lightning

*¿Quién controla mi **bitcoin**?*

Monederos Auto-Custodiales

- *Beneficios:*
  - Es la única forma de convertirse en el dueño absoluto del ***bitcoin*** que se ha comprado.
  - No es necesario pedir permiso para usar el servicio.
  - No hay un proceso de aprobación de cuentas.
  - Cualquier persona del mundo puede descargar la aplicación y usarla de inmediato.
  - Es como tener el dinero guardado en casa en lugar de confiárselo al banco.
  - La autocustodia de nuestro ***bitcoin*** es muy recomendable para evitar robos.
  - Ninguna empresa/gobierno tiene control/autoridad sobre las transacciones.
  - Ningún tercero puede confiscar arbitrariamente lo que está en autocustodia.
  - En momentos de estrés, tenemos la seguridad que nuestro ***bitcoin*** está a salvo.

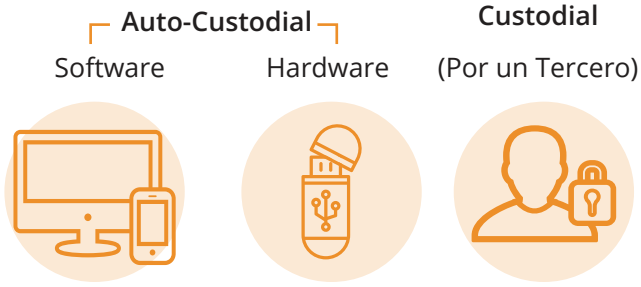
- *Riesgos:*
  - No hay manera de recuperar los fondos en caso perder las **claves privadas**.
  - Menos acceso a servicio al cliente
  - La responsabilidad no está distribuida

Monederos Custodiales

- Un tercero guarda tu ***bitcoin***.
- Los fondos (las **claves privadas**) están bajo el control del proveedor del monedero.

- *Beneficios:*
  - Si pierdes u olvidas el acceso a tu cuenta, se recupera el dinero fácilmente.

- *Riesgos:*
  - Siempre conectados al internet, lo que los hace más vulnerables.



Compra, Custodia y Movimiento de Bitcoin

¿Cuál es el monedero más conveniente?

- **Monederos Hardware [Fríos]**
  - Monederos "*no conectados*", ya que como su nombre lo indica, no requieren internet para funcionar.
  - Son los monederos más seguros en existencia.
  - Ideal para almacenar grandes cantidades de ***bitcoin***.
  - Sus claves se almacenan en un dispositivo de hardware. [Ej.: Coldcard MK3.]
  - La pérdida del monedero sin copia de seguridad resulta en fondos irrecuperables.

- **Monederos de Papel [Fríos]**
  - Las claves privadas se copian en un papel como forma de protección.
  - Una de las formas más seguras pero extremadamente ineficiente para almacenar ***bitcoin***.
  - Es necesario copiar una nueva **clave privada** cada vez que se realice una transacción.

- **Monederos Software [Calientes]**
  - Conectados al internet.
  - Se puede instalar y/o acceder a través de una aplicación en el móvil o vía web.

  - **Monederos Móviles**
    - Portable y conveniente; ideal cuando se hacen transacciones cara a cara.
    - Los mercados de aplicaciones los podrían eliminar sin preaviso.
    - Si el dispositivo se daña o se pierde, puede ser difícil recuperar los fondos.
      - Ideales para usar con códigos QR.

  - **Monederos de Escritorio**
    - Los usuarios pueden tener control completo sobre los fondos.
    - Algunos ofrecen soporte a monederos fríos.
    - Difícil de utilizar códigos QR al realizar transacciones.
    - Susceptible a los virus que roban ***bitcoins***.

Arquitectura de los Monederos Bitcoin

Seguridad		FÁCIL	DIFÍCIL
	ALTA	Monederos Fríos Custodiales	Monederos Fríos Auto-Custodiales
	BAJA	Monederos Calientes Custodiales	Monederos Calientes Auto-Custodiales
		Facilidad de Uso	

¿Cómo envió o recibo satoshis?

- **En-cadena** (***on-chain***):
  - A través de monederos conectadas a la red "principal".
  - Esta es una forma muy segura pero muy lenta-hasta 10 min. para confirmar la transacción.
  - Las comisiones de cada transacción son proporcionales su tamaño digital, no a su monto.
    - Si envías un valor de 1$USD en cadena, y se paga $1 en tarifas, esto representa el 100%.
    - Si envías 10,000$USD en cadena, y se paga $1 en tarifas, esto representa el 0.01%.

- **Lightning Network** (***off-chain***):
  - Una solución de "capa 2"- permite enviar y recibir ***bitcoin***.
    - *Pagando tarifas muy bajas o sin tarifas y de manera excepcionalmente rápida.*
  - Se utilizan en países donde:
    - *Las políticas y regulaciones loca les fomentan la adopción masiva.*
    - *Se requiere una solución de transacción rápida, privadas, económica y eficiente.*

5.3 El Ciclo de una Transacción *(on-chain)*

¿Qué es una transacción de Bitcoin?

Lo que se envía y se guarda a través del protocolo **Bitcoin** es ***bitcoin***, no son pesos ni dólares.

- A esta transferencia de dinero es lo que se le llama una ***transacción***.

- Un traspaso de valor entre dos monederos, el cual queda grabado en la blockchain (**Bitcoin**).

Cuando una nueva transacción ingresa a la red:

- Debe pasar un proceso de verificación para ser aceptada por los nodos
  - Las transacciones ***válidas:***
    - Se transmiten de una computadora a otra hasta que todas tengan copia.
    - Aproximadamente cada diez minutos se agrupan miles de transacciones.
    - Se crea un nuevo bloque, a través de un proceso llamado ***minería***.
    - Las nuevas transacciones quedan grabadas en el bloque para siempre.
    - Será imposible modificarlas, borrarlas o agregarles información.
  - Las transacciones ***inválidas:***
    - Simplemente se rechazan y no se propagan por la red.

Puentes y Paradas para realizar Transacciones y Guardar BTC

Una transacción a través de un monedero se asemeja al siguiente proceso:

- Imaginemos como si todo el ***bitcoin*** en existencia estuviese guardado cajas de seguridad.
  - Todas con diferente cantidad de BTC, pero completamente transparentes.
  - Cualquiera pudiese ver cuanto ***bitcoin*** hay en cada caja y el historial de cómo llegó allí.

- Cada caja tiene una ***dirección*** perteneciente a un sólo dueño.

- Esta dirección está protegida con un candado de seguridad, el cual necesita dos llaves diferentes:
  - Una de las llaves, la llave privada, ***abre*** el candado y ***da acceso al BTC adentro***.
  - Y la otra llave, la llave pública, ***cierra*** el candado y ***protege el BTC***.

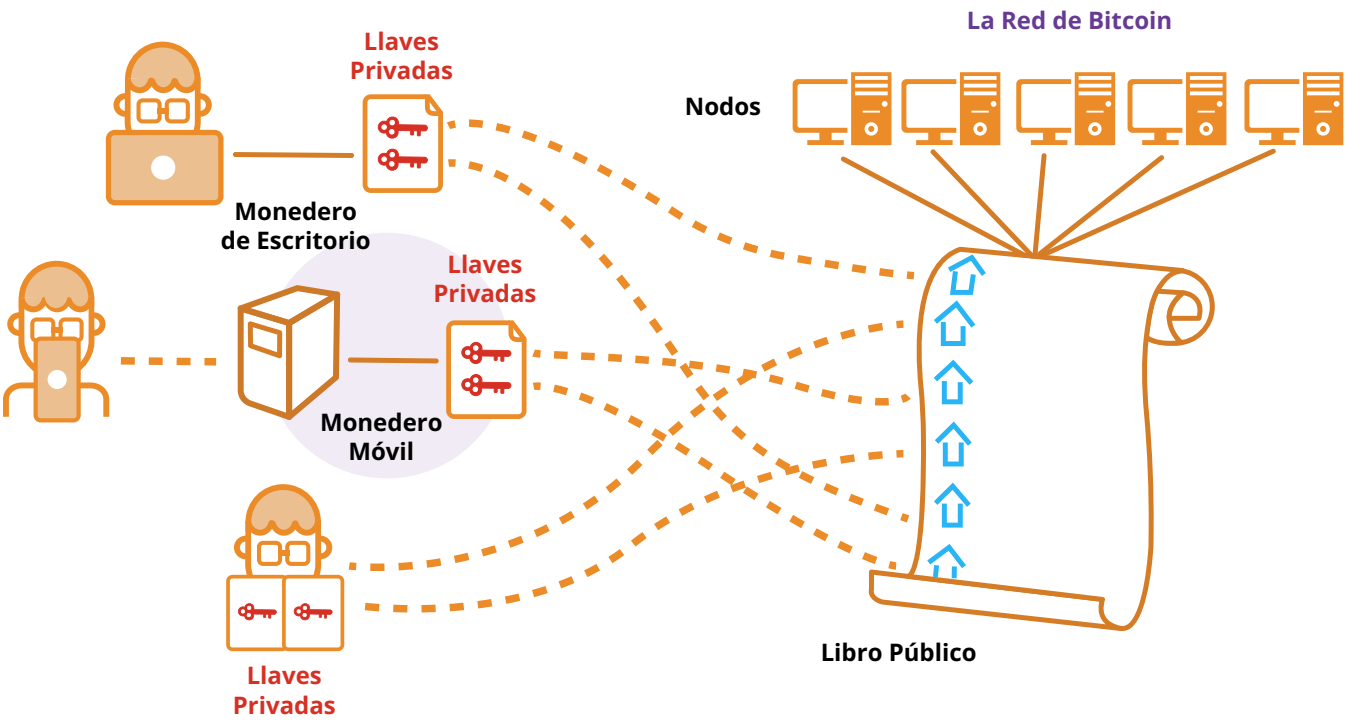
- Cada participante en la red ***guarda*** sus llaves privadas en lugares muy seguros.

Compra, Custodia y Movimiento de Bitcoin

- Si una caja tiene ***bitcoin***, el dueño en cualquier momento puede abrir su caja para:
  - Trasladar cualquier cantidad de fondos deseados a otra caja diferente.
  - Pero antes, tomando en cuenta que existen miles y miles de cajas:
    - -Necesita una dirección exacta, para garatizar que se va a depositar el BTC a la caja correcta.
  - Por último, se debe cerrar el candado de caja fuerte con la llave pública del recipiente.
    - - Para que nadie, fuera del destinatario, tenga acceso al ***bitcoin***.
  - En el futuro, la caja sólo se podrá abrir con la llave privada de quién recibió el BTC.

¿Cómo funciona una transacción paso a paso?

El éxito de transferir dinero en una red descentralizada solo se logró bajo la premisa que cada transacción es única y reconocible.



● Supongamos que Carlos va a enviar 0.5 bitcoin a su hermana Laura. Ambos tienen monederos.

• Es necesario crear una transacción que lleve un ***identificador único e irrepetible.***

- Este identificador es la ***huella digital*** de cada transacción.
- Esto es así para evitar que dos transacciones pasen por ser idénticas.
- Y esto también hace que el proceso de verificación sea sencillo.

- Para que esto suceda de manera segura pero eficiente, se requiere cifrar, descifrar, firmar y verificar cada transacción.

▫ **Cifrar:** Carlos tiene que enviar el ***bitcoin*** a través de un canal seguro sin que nadie lo intercepte.

▫ **Descifrar**: Laura tiene que recibir el dinero, asegurarse que nadie más tenga acceso a él y poder usarlo.

▫ **Firmar**: Carlos tiene que comprobarle a Laura que el dinero que envió si le pertenecía a él originalmente y que está mandando la cantidad correcta.

▫ **Verificar**: Los usuarios en la red tienen que verificar que Carlos si tenía ese dinero en su cuenta para gastar, lo tienen que deducir de la cuenta de Carlos, y agregarlo a la cuenta de Laura.

Veamos como sucede:

● **1.** Carlos abre su monedero en su celular y le pide la dirección de envío (llave pública) a Laura.

● **2.** Laura se la comparte (*en forma de código QR, correo electrónico u otros métodos).*

● **3.** En esta transacción, Carlos escanea el código QR y lo vincula a la cantidad que enviará.
- Agregando una comisión pequeña como incentivo para que los ***mineros*** la seleccionen.

● **4.** Con un click, se verifica si Carlos tiene suficiente fondos en su monedero.

● **5.** El monedero de Carlos ***firma*** la transacción con su llave privada.
- Su ***bitcoin*** se vuelve disponible para Laura.

● **6.** La transacción se transmite a través de la red a los ***nodos*** para ser ver si es aprobada.
- Después de ser verificada, permanece en un área de espera.

● **7.** Los ***nodos mineros*** seleccionan miles de transacciones y rechazan las inválidas.
- Las agregan a nuevos "*bloques candidatos*", los cuales todavía no han sido aceptados.
- Comprimen toda la información y cada uno crea un identificador de bloque.

● **8.** Comienza una competencia entre ***nodos*** (similar a una rifa entre identificadores de bloque).
- Para ver a quién es el próximo en agregar su bloque a la cadena de bloques.

● **9.** El bloque ganador contiene la transacción de Carlos-Laura y lo propaga a otros nodos.

● **10.** Los nodos verifican el identificador del bloque ganador y lo agregan a la cadena de bloques.
- Todas las transacciones en dicho bloque quedan ***confirmadas*** en la cadena de bloques.
- No habrá forma de modificar o borrar; quedará registrado para siempre en su lugar.

● **11.** Laura se convierte en el propietario acreditado de ese ***bitcoin***.
- Habrá recibido sus 0.5 BTC en aproximadamente 10 minutos.
- Carlos lo verá restado del balance de su ***monedero***.

● **12.** La transacción habrá terminado con éxito.

UTXO - "Monedas no Gastadas"

Las transacciones son simplemente ***entradas*** y ***salidas*** de ***bitcoin*** de un monedero a otro.

● Todo bitcoin que todavía no se haya gastado se considera ***UTXO***, *unspent transaction output*, o monedas no gastadas.

● El ***estado actual*** de la cadena de bloques es la base de datos ***UTXO***.

● Las ***entradas*** se refieren al dinero que se usa para ***generar una transacción***.

● Las ***salidas*** indican generalmente dos puntos a los que se ***dirige la transacción***:
- Una salida va a la persona a la que se realiza el pago.

● Cuando un usuario desbloquea su UTXO con su clave privada para enviarle a otro,
- Su saldo puede estar en peligro, ya que su caja de seguridad está abierta.
- Por este motivo, es recomendable siempre mandar cualquier saldo a un monedero nuevo.

- Si el *monedero* original tiene un saldo:
  - La otra salida se dirige a una dirección nueva creada para recibir el cambio.
    - Convirtiendo esta cantidad en una entrada nueva ***UTXO***.

- Para los nodos en la red, es fácil llegar a un consenso ya que:
  - Todos mantienen una copia de la misma base de datos
  - Pueden comprobar los saldos de cada una de las direcciones.

La Confirmación de una Transacción

- Para autorizar y ***enviar*** cualquier ***salida*** de ***bitcoin*** de un monedero,
  - Se debe ***firmar*** la transacción con la clave privada.
  - Este paso es necesario para probar que uno es propietario de sus fondos.

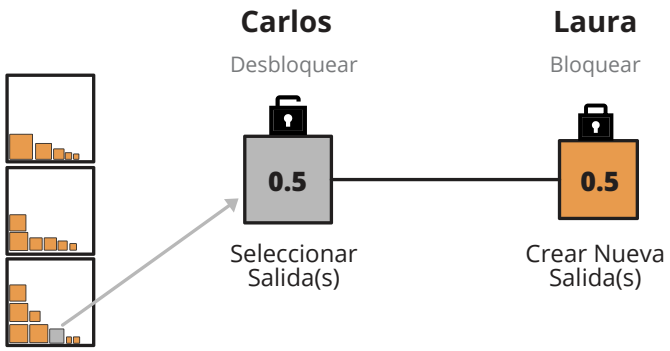
- Para ***recibir*** una ***entrada*** a un monedero:
  - Un usuario debe haber compartido su ***dirección*** con el emisario.

- La transferencia se ***CONFIRMA*** cuando:
  - **Bitcoin** ***ha apuntado*** la cantidad de ***bitcoin*** que se depositó a ***la nueva dirección***.
  - Y la ***ha restado*** del monedero ***de quien lo envió.***

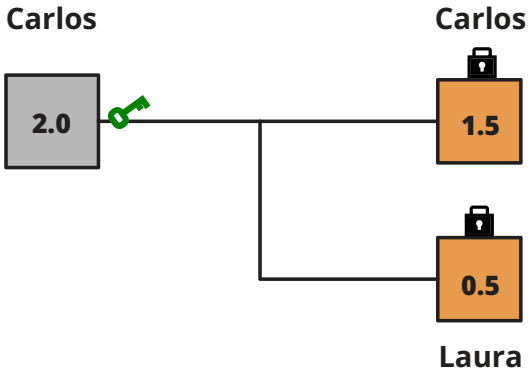
*Veamos cómo se **confirma** una transacción:*

- Las cajas amarillas representan UTXO

- Las cajas grises representan monederos en los que ya no hay ***bitcoin*** (completamente vacías).



- El nodo confirma que sí había suficiente ***bitcoin*** apuntando a la dirección original (0.5 BTC en el monedero de Carlos) para ejecutar la transacción.
- Cuando se confirma la transacción, se ha repartido cierta cantidad de ***bitcoin*** a dos direcciones diferentes.
- Algunas cajas ahora tienen más ***bitcoin*** (la de Laura), y la original (la de Carlos) tiene menos.



- Después de haber confirmado la transferencia, la blockchain solo se encargará de monitorear los monederos que recibieron dinero, el de 1.5 BTC, y el de 0.5 BTC.

- Este es ahora el ***bitcoin*** no gastado o el ***UTXO***.

Clase #6

Bitcoin cómo Depósito de Valor y Red de Pagos

6.1 El Problema del Doble Gasto
6.2 Grupo de Memoria o “Mempool”
6.3 Transacciones Verificadas, pero No Confirmadas
6.4 La Red de Bitcoin (On-Chain)
- Nodos Completos
- Actividad: Estado de las Transacciones

6.5 “Lightning Network” (Off-Chain)
- ¿Cuál es la diferencia entre la Capa 1 y la Capa 2?
- Actividad: Como funciona el Lightning

6.1 El Problema del Doble Gasto

Antes de entrar en detalle, contemplemos lo siguiente:

- **Bitcoin es dinero digital**. Esto significa que a diferencia del dinero convencional:
  - No puede duplicarse como otro tipo de archivos digitales (fotos, videos, etc.),
  - No puede ser *replicado*, *falsificado* y/o *enviado a múltiples personas* simultáneamente.
  - No puede ser facturado como un cobro doble a través de una tarjeta de crédito.

¿Qué beneficios trae esta característica de bitcoin? Expliquemos con un ejemplo.

- Es común que las personas almacenen sus recibos y/o mantengan un registro de sus gastos.
  - Periódicamente comparan sus cuentas con los saldos bancarios y verifican que no haya ninguna discrepancia de gastos.

- Por ejemplo, alguien puede darse cuenta que un restaurante cobró su tarjeta de crédito dos veces:
  - Hay dos retiros de $5.08 del miércoles 26 de enero de 2022.
  - Le han facturado doble por el mismo almuerzo.
  - Probablemente va o llama al banco para tratar de revertir uno de los pagos.
  - En el mejor caso, si el banco acepta su disputa, recuperará su dinero en unos meses.
  - En el peor de los casos, el restaurante se opone a devolver el dinero alegando que hubo dos compras.

- Sigamos explorando ejemplos del día a día para ilustrar la idea del "***doble gasto***":

  - **Día #1**: Digamos que Raquel pide un almuerzo en McDonalds por $10 USD.
    - *Paga en efectivo con dos billetes de $5.*
    - *El pago queda confirmado al instante.*
    - *Ambas partes han presenciado físicamente el trámite.*
    - *Ha sido un intercambio sencillo, una hamburguesa a cambio de dinero.*

  - **Día #2**: Raquel pide el mismo almuerzo y tiene dos billetes de $5 USD de nuevo.
    - *Pero uno es original y otro falso (una copia exacta). Los entrega como forma de pago.*
    - *Siendo los números de serie idénticos, el cajero fácilmente podría ver que uno es falso.*
    - *O simplemente aceptarle el pago como el día anterior.*
    - *El cajero, estando en una jornada ajetreada, acepta el pago sin ver los billetes.*

  - **Día #3**: Raquel estuvo de buenas, pero le da miedo volver a McDonalds.
    - *Ahora, va a tratar de replicar su **bitcoin** como replicó su billete en McDonalds.*
    - *Ella le debe 0.2 BTC tanto a Jaime como a Pepe, pero sólo tiene 0.2 BTC en su monedero.*
    - *Raquel abre su monedero en su teléfono y en el de su mamá, con frase semilla.*
    - *Desde su teléfono personal manda los 0.2 BTC a Jaime.*
    - *Desde el teléfono su mamá manda 0.2 BTC a Pepe.*
    - *Se asegura de mandar las dos transacciones exactamente al mismo tiempo.*

- *Dos nodos diferentes reciben las dos transacciones.*
- *Recordemos que Raquel tenía sólo 0.2 BTC en su monedero para gastar.*

- ¡Los nodos de la red se dan cuenta y una de las dos transacciones se rechaza!

- ¿Pero cómo? Si tenemos un sistema en el que ningún computador está a cargo, ¿cómo se hace para decidir cuál transacción se rechaza y cuál queda escrita inalteradamente en la cadena de bloques?

- Para lograr esto, Satoshi Nakamoto logró encontrar un mecanismo exitoso que:
  - Revisa si una transacción es válida o no, de manera consensuada entre todos los participantes en la red, antes de agregarla en la cadena de bloques.
  - Una solución ingeniosa a problemas como los mencionados anteriormente.

¿Cómo funciona?

6.2 Grupo de Memoria o "Mempool"

- Antes de que cualquier transacción se pueda ejecutar y fijar en un bloque,
  - Entrará a un área de espera llamada "***mempool***", o grupo de memoria.

¿Qué es y que sucede con las transacciones que entran aquí?

- Un sitio donde existen miles de transacciones verificadas pero no confirmadas.

- No existe una *mempool global*; cada uno de los nodos debe:
  - Verificar la validez de las transacciones antes de incluirlas en su ***mempool***.
  - Propagar transacciones verificadas a los nodos vecinos.
  - Rechazar transacciones inválidas.

Aquí se puede observar cómo se dispersan rápidamente las transacciones válidas de nodo a nodo.

- Los nodos deben decidir si las transacciones son válidas o no.
  - Si son aceptadas:
    - Esperan que un minero la seleccione y las adicione en el siguiente bloque.
    - Eventualmente se graban *permanentemente* en la base de datos compartida.
  - De lo contrario, se pueden rechazar si:
    - Existe un conflicto con otra transacción.
    - Si no hay suficientes fondos para transferir.
    - Si la firma no es válida y no puede comprobar que se puede gastar dicho BTC.

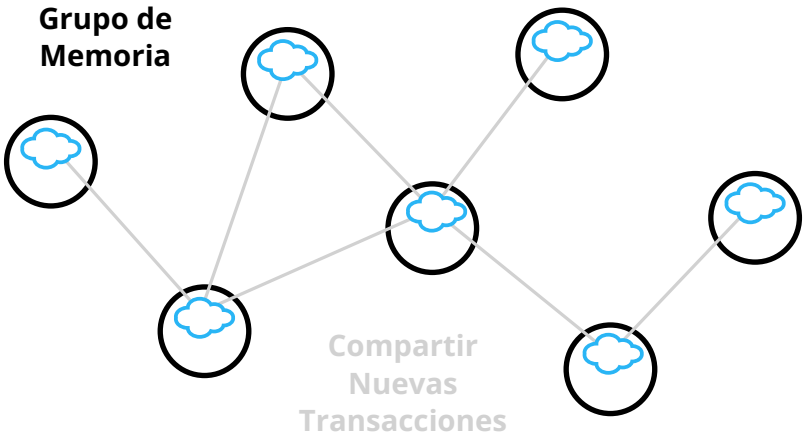
• Algunas transacciones simplemente se quedan en el área de espera.

- Por hasta 72 horas, hasta que por fin se rechazan, ya que no agregan un incentivo monetario suficientemente atractivo.

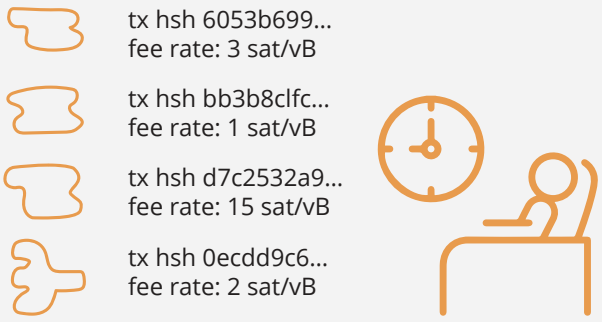
● La mempool proporciona una capa adicional de seguridad y resistencia contra los ***ataques DDoS***.

• Cuando una red se inunda con transacciones minúsculas.

- Provocando una congestión in manejable.



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



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.

El objetivo principal de un *mempool* es:

1 Transmitir transacciones no confirmadas.

2 Proporcionar a los mineros transacciones para que puedan minar.

6.3 Actividad: Transacciones Verificadas, pero No Confirmadas

Actividad de Clase. Sigue las instrucciones del maestro para realizar esta actividad. Ingresa al enlace con el código QR para empezar.

- A continuación podemos ver una transacción real sin confirmar:
  - Un identificador único (*la huella digital de la transacción*).
  - El espacio de memoria que ocupa.
  - La comisión que se paga.
  - El monto de la transferencia.

TxID: a434948b2de9de18398294f84e42436ec59fb86faf34a21052bd640a97cd94b7d

_____ input ➡ _____ outputs

Size: _____ vbytes *(Espacio de memoria que ocupa)*

Fee Rate: 27.01 sats/vbyte *(Tasa de Comisión / vbyte actual)*

Fee: _____ sats *(Comisión de la transacción)*

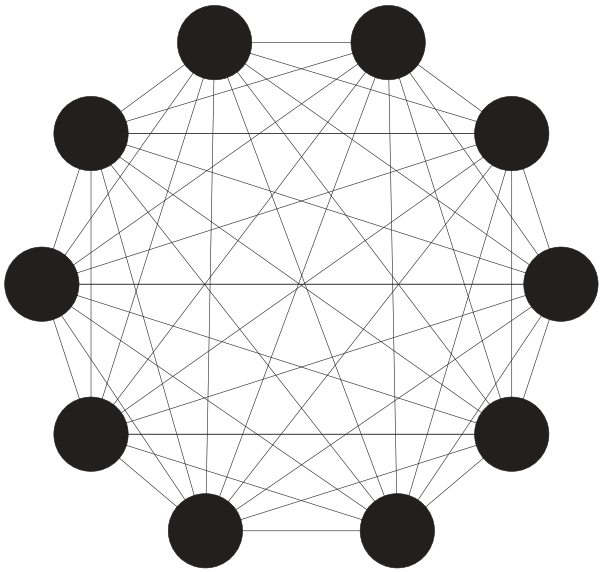
Total Value: ₿ _____ BTC ≈ $ _____ USD *(Valor total de la transacción)*

- *¿Podríamos analizar otra u otras transacciones?*
  - ¿Es de mayor o menor monto?
  - ¿Los participantes pagaron una comisión más alta o más baja?
  - ¿Cuál transacción será más probable encontrar en el siguiente bloque? Porqué?
  - ¿Qué querrá decir cuando un bloque se cae hacia el abismo?
  - ¿Qué quiere decir cuando se confirma una transacción?

6.4 La Red de Bitcoin (On-Chain)

- Está compuesta por los nodos de **Bitcoin**.
  - Aquellos equipos computacionales que se adhieren a un sistema de reglas (*Bitcoin Core*).
    - Se comunican entre sí a través del ciberespacio convirtiéndolos en una red.
    - Cada uno de los cuales ejecuta su propia versión del software **Bitcoin**.

La Red de Bitcoin
Nodos conectados siguiendo un conjunto de reglas en común.

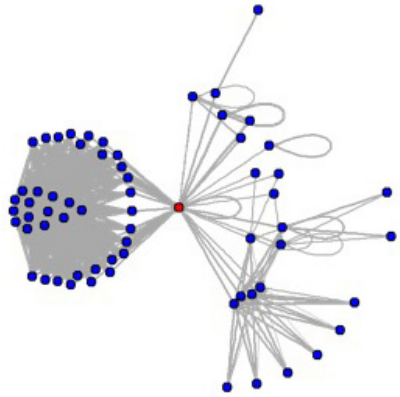


- Desde estos puntos de conexión se puede crear, enviar, y recibir información (i.e. transacciones).
  - Existen diferentes tipos de nodos; cada uno ejerce un papel diferente en la red.

Nodos Completos

- Ejecutan el software de **Bitcoin.**
  - Tienen autonomía de tomar sus propias decisiones, sin embargo, a través del consenso:
    - Toman las mismas decisiones, convirtiéndolos en una red descentralizada confiable y segura.
    - Los nodos completos tienen tres diferentes funciones:

▫ **1. Compartir información** *(a sus nodos vecinos).*



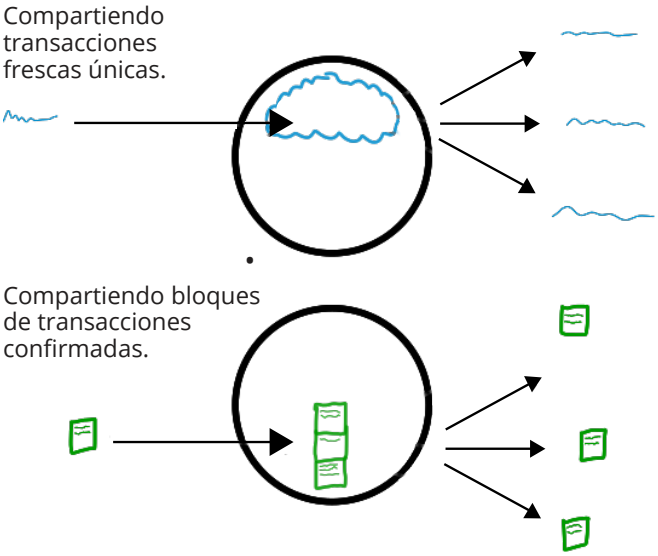
Este diagrama representa la propagación de una transacción.

• Hay dos tipos de transacciones que comparten los nodos:

— **A. Transacciones Frescas**
- Estas van directamente a la *mempool*.
- Los nodos se encargan de verificar o rechazar estas transacciones.
  - Se basan en el historial de la *blockchain* y el conjunto de reglas del software.
- Retransmiten las transacciones válidas a sus nodos vecinos.
  - Nadie quiere recibir transacciones defectuosas o maliciosas.

— **B. Transacciones Confirmadas**

- Transacciones que han sido "*confirmadas*" y escritas en un bloque.
- Estas se agrupan y forman los bloques; no se comparten individualmente.



▫ **2. Guardar una copia de las transacciones confirmadas.**

• Mantienen una copia completa de todos los bloques en la cadena de bloque,
• Cada *confirmación* reduce exponencialmente el riesgo de que la transacción sea revertida.

▫ **3. Validar los bloques y llegar a un consenso con los otros nodos.**

• Todos los nodos participantes deben aceptar unánimemente la información que contiene un bloque entero antes de incluirlo en la cadena de bloques.
• Una copia de la cadena de bloques para su custodia y la comparte con otros nodos.

● El estatus de sus transacciones frescas y confirmadas se pueden localizar en la red. *¿Cómo?*

• Los exploradores de bloques son una ventana a todas las transacciones cadena de bloques
• Permiten comprobar el saldo de cada dirección, ver los detalles de cada tran=sacción y más.

Actividad: Estado de las Transacciones

Actividad de Clase. Vamos al siguiente enlace donde podemos observar diferentes propiedades de las transacciones.

https://www.blockchain.com/explorer?view=btc

Termina de responder las preguntas en la siguiente hoja.

En el enlace de *blockchain.com*, podemos observar todo lo siguiente:

- El monto total que se transmite.
- Cuantas entradas y salidas hay.
- El tamaño *(o la memoria que ocupa en el bloque).*
- El ID de una transacción aleatoria.
- El estado de la transacción.
- Si la transacción ya ha sido confirma da, y muestra el número total de confirmaciones hasta el momento.

¿Qué información reconoces? ¿Cuál te sorprende? ¿Cuál es el valor de la última transacción? ¿Podemos ver si ya está confirmada?

- No todos los usuarios tienen suficiente espacio en su disco duro para convertirse en un nodo.
  - De ser ese el caso, simplemente se puede descargar un monedero y realizar transferencias o guardar BTC a largo plazo.

6.5 "Lightning Network" (Off-Chain)

¿Cuál es la diferencia entre la Capa 1 (o Capas Base) y la Capa 2?

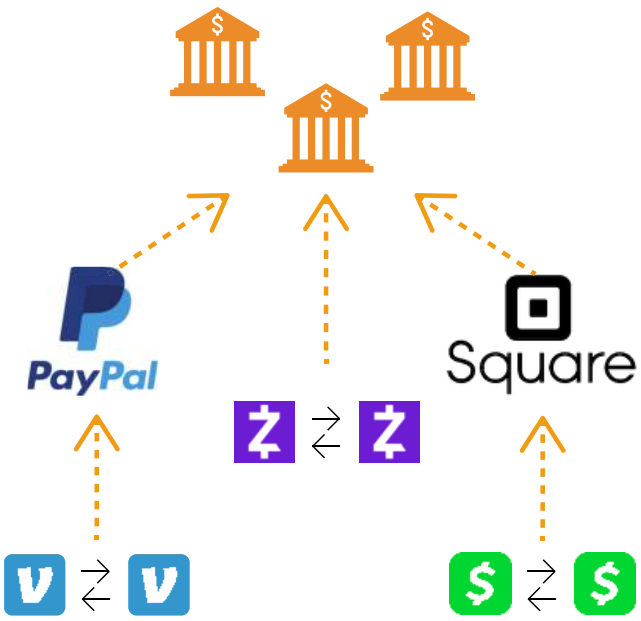
¿Qué haces con una carretera segura pero congestionada? Simple, conectas una carretera para descargar el tráfico. Esta es exactamente la diferencia entre las redes *blockchain* de Capa 1 y Capa 2.

- Muchas piezas tecnológicas importantes de **Bitcoin** e incluso muchas transacciones no ocurren dentro de la "cadena de bloques".

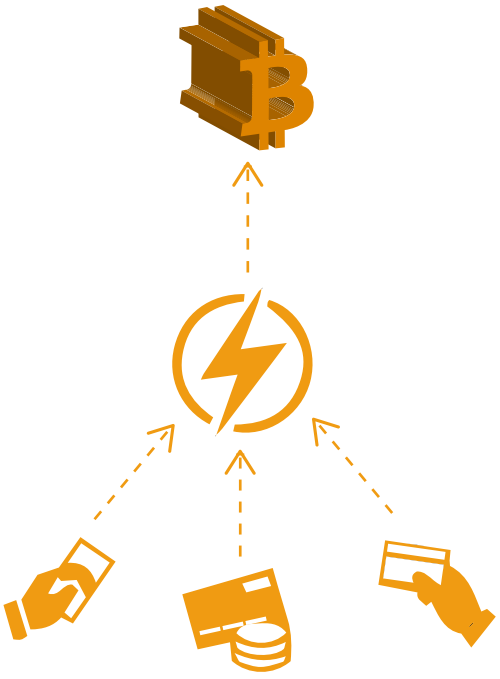
- **Bitcoin** es revolucionario ya que es la *capa base* del *internet descentralizado*.
  - Pero tiene un problema fundamental de escalabilidad.
  - Las transacciones de **Bitcoin** pueden ser lentas y caras.
  - Se argumenta que ***bitcoin*** no se puede usar como medio de pago por ser lento y caro en micro pagos.
  - Existen transacciones de US$1 o US$2 que terminan costando más de US$5 cuando se usa la red principal.
  - Visa procesa hasta 65.000 transacciones por segundo (tps), mientras que la red **Bitcoin** solo puede manejar 7/tps.

- Ahí es donde la magia de las *soluciones de **capa dos***, como ***Lightning***, ha venido al rescate.
  - Con ***Lightning Network***, ***bitcoin*** tiene el potencial de ser la moneda de la era digital.
    - Rápida
    - Inmutable
    - Descentralizada

Sistema Monetario Moderno = Redes Cerradas
Los bancos mantienen la finalidad



Sistema Monetario Bitcoin = Red Abierta
Bitcoin mantiene la finalidad



Todas las aplicaciones creadas en **Lightning Network** son interoperables

- ***Lightning***, es un conjunto de reglas (*contratos inteligentes*), construido encima de **Bitcoin**:
  - Que permite transacciones instantáneas.
  - De alto volumen.
  - Desconectadas de la red principal.
  - No es necesario registrar todas las transacciones en la red.
    - Sino en una red alterna más eficiente.
    - Brinda toda la seguridad de **Bitcoin** sin algunos de sus inconvenientes.
      - Pero con diferentes tipos de compensaciones.
  - Ofrece más privacidad.
  - ***Lightning*** aborda los problemas de escalabilidad de **Bitcoin**.

- Analicemos la siguiente analogía:

  - Un huésped se registra en un hotel; de anticipado le piden su tarjeta de crédito.
    - Para cubrir los cargos de habitación y tarifas imprevistas de la estadía.
  - Es *más eficiente y menos costoso* que cargar la tarjeta cada vez que incurre en un gasto.
  - El hotel lleva un registro de todos los gastos del cliente.
  - Existe una farmacia y una peluquería independientes dentro del hotel.
    - El huésped compra productos, usa servicios y firma la deuda a su habitación.
    - El hotel cobra una comisión por inter mediar el pago entre el huésped y el negocio.
  - Si el huésped tiene algún problema o una queja, se le descuenta la cantidad necesaria de su cuenta.
  - La tarjeta sólo se carga después de la estadía, cuando el huésped haya verificado que los cargos y el saldo sean correctos.

Bitcoin cómo Depósito de Valor y Red de Pagos

Aprendamos más sobre el Lightning Network y sus beneficios.

Lightning Network funciona de manera similar a la analogía pero diferente. *¿Cómo así?*

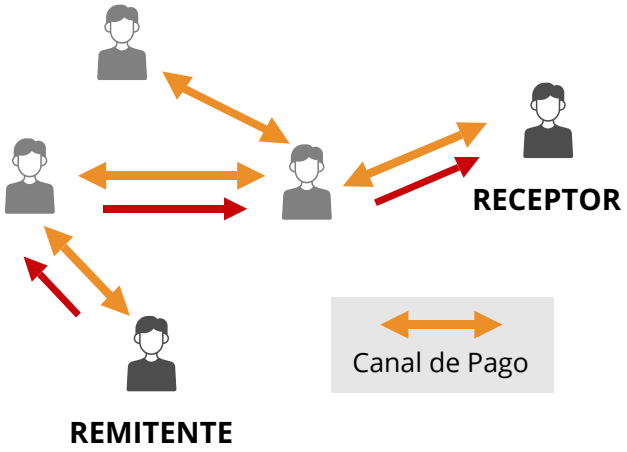
- La analogía es precisa con la exclusión de la necesidad de confianza
  - Este es un malentendido muy común de ***Lightning***: *no es un sistema de crédito.*
  - Las transacciones de ***Lightning*** no son pagarés:
    - Son transacciones de **Bitcoin** válidas que mueven *UTXO reales*.

- En lugar de darle a alguien una tarjeta de crédito y dejar una cuenta abierta.
  - Dos nodos pueden abrir un *canal de pago*, o una ruta de transferencia.
  - Las partes pueden realizar transacciones veces tantas como lo deseen.
    - Manteniendo su saldo siempre actualizado.
  - Cuanto más grande un canal,
    - Mayor la cantidad de ***bitcoin*** que se puede transferir en ambas direcciones.
  - Se puede construir rutas con todos aquellos con los que se hacen transacciones.
  - Cuantos más canales,
    - Más conexiones y mejores atajos para llegar a ciertos destinos.
  - Si existe una ruta directa,
    - Todo es sencillo y se hace una transaccion según el tamaño del canal.
  - Si la conexión es a través de un tercero (un puente),
    - Se paga un *peaje* por pasar.
  - Para abrir un canal nuevo, ambos nodos pagan un fee pequeño a los mineros.
  - No se necesita actualizar y verificar cada transacción en la red.
    - Esto sería costoso y tomaría mucho tiempo.
    - Por el contrario, se aprueba cada movimiento con ambas firmas digitales.
  - Cuando cualquiera de las partes decide cerrar el canal,
    - Puede transmitir unilateralmente la última transacción a la red **Bitcoin**.

Mira una visualización en el siguiente enlace:

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

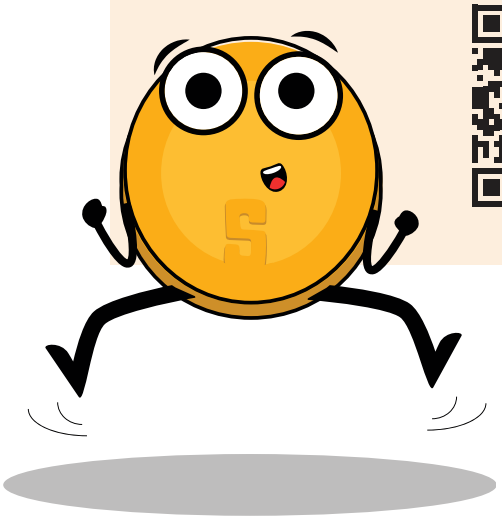
- Si **A** tiene un canal abierto con **B** y **B** tiene un canal abierto con **C**, **A** puede enviar BTC a **C** a través de **B,** sin necesidad de confiar o conocer a **B**.



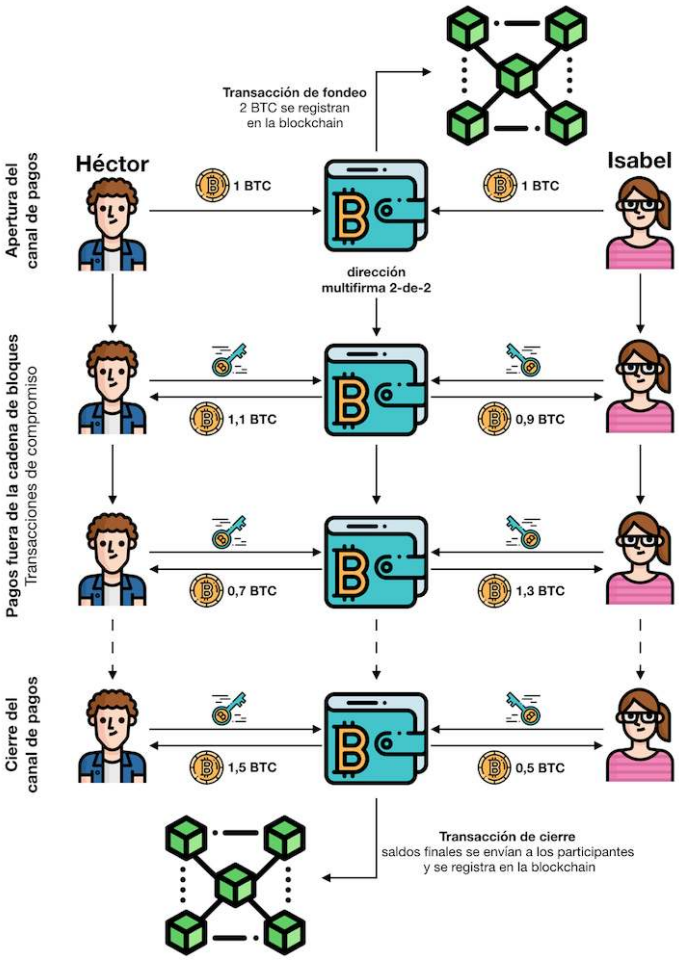
Actividad: Como funciona el Lightning

Actividad de Clase. Vamos a ver un simulador. Espera instrucciones del maestro para completar esta actividad.

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

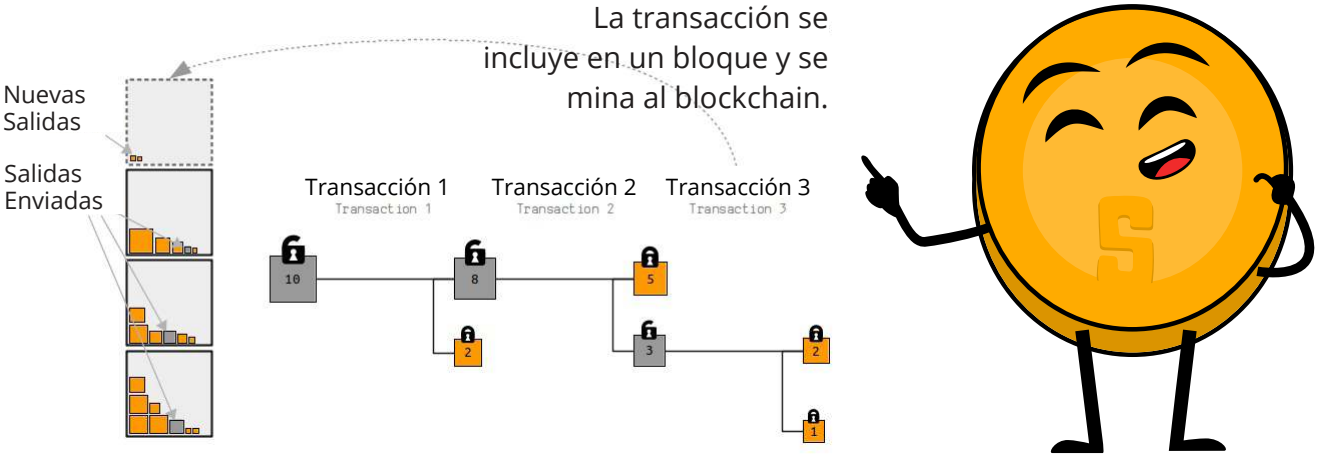


- El uso de ***Lightning*** es tan barato y rápido como el envío de un correo electrónico.
  - Con el beneficio adicional de la naturaleza segura y sin confianza de **Bitcoin**.
  - Sólo las dos personas que mantienen dinero en un canal abierto saben *cuánto, qué tan a menudo y cuándo se mueve ese dinero*.

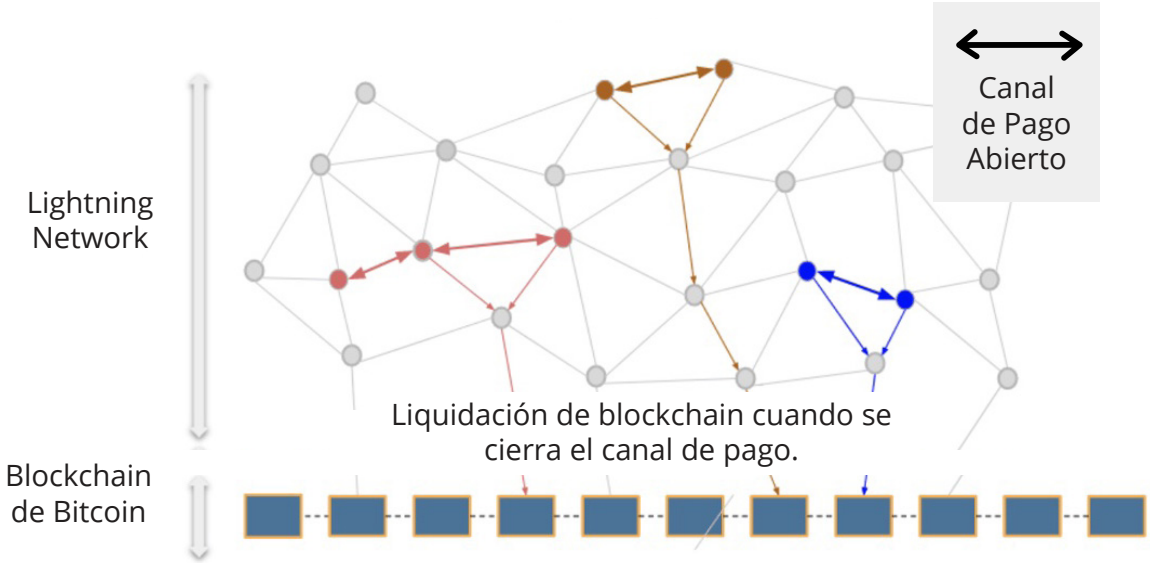


- En comparación, si se hacen tres transacciones "en cadena", es decir, *si se quedan en la **capa base***:
  - Las transacciones hubieran sido mucho más lentas y caras.

• Cada una de estas transacciones tendría que involucrar a todos los participantes de la red.
• Se podría visualizar de la siguiente manera:



Cómo funciona Lightning Network:



Clase #7

Los Mineros y la Minería de Bitcoin

7.1 Los Nodos Mineros
- ¿Cómo es la competencia matemática entre mineros?

7.2 Un Pequeño Desvío- Para entender los hashes
- ¿Qué es una función?
- ¿Qué es un hash?
- ¿Qué es SHA 256?
  - Actividad: Creando Hashes
- ¿Qué es un “nonce”?
- ¿Qué es un Árbol de Merkle?

7.3 La Minería
- No Confíes, Verifica
- El Hash del Bloque
- El Nonce del Bloque
- Actividad: Analizar Bloques en Tiempo Real

Los Mineros y la Minería de Bitcoin

7.1 Los Nodos Mineros

- Se esfuerzan por ser los primeros en resolver problemas matemáticos y crear nuevos bloques.
    - Con el objetivo de ganar recompensas monetarias.
    - Y la condición de demostrar que han trabajado por ello.
    - Por lo tanto, ayudado a mantener la red segura.

- Los mineros siempre ejecutan un nodo completo, pero también:
    - Empaquetan las transacciones válidas en grupos, creando y proponiendo bloques.
        - A través de un mecanismo que le da seguridad a la red llamado *Proof of Work, PoW (de ahí el nombre "prueba de trabajo", en inglés proof-of-work)*.
        - Es necesaria para la seguridad, lo que previene el fraude y permite la confianza dentro de la red.

- La recompensa de cada bloque consiste en:
    - Nuevo ***bitcoin*** fabricado por el software de **Bitcoin**.
    - Y las comisiones incluidas por las transacciones incluidas en dicho bloque.

- Una diferencia clave entre los *nodos completos* y los *nodos mineros*:
    - Los *nodos mineros* pueden proponer nuevos bloques a la red **Bitcoin**.
    - Tratan de resolver rompecabezas criptográficos en un proceso llamado "*minería*".
    - Deben demostrar que ellos son los que han realizado el trabajo requerido.
    - Por lo tanto, pueden recibir *recompensas* por los bloques.
    - Los *nodos completos* no pueden proponer bloques nuevos
    - Por lo tanto, *no* pueden recibir recompensas.

¿Cómo es la competencia matemática entre mineros?

- De nuevo volvamos a una analogía:

○ Cada minero tiene un dado especial que tiene marcados los números 1 hasta el 1000, es decir, tiene 1,000 caras.
○ Los mineros se alistan para entrar a una competencia, con el incentivo de ganar un poco más de 6.25 ***bitcoin*** en los próximos 10 minutos.
○ **Bitcoin** escoge un número objetivo del 1-1000 y lo publica para que todos lo vean en la red. Digamos que escoge el #8. Empieza la competencia.
○ El objetivo final es caer en un número menor a 8.
    - Algunos mineros tienen ventajas y una probabilidad mayor de ganar. ¿Porqué?
    - Tienen más poder adquisitivo y han comprado más de un dado.
    - Otros lanzan a una velocidad mayor que otros.

○ Comienza la competencia:
    - Los mineros empiezan a lanzar su dado cientos de veces pero esto requiere de mucho trabajo. Se les cansa la mano.
    - Un minero afortunado alza la mano y dice "¡gané!".
    - Todos los otros mineros paran de lanzar sus dados y miran la mesa en la que están jugando.
    - De esta manera, todos pueden verificar si está diciendo la verdad.

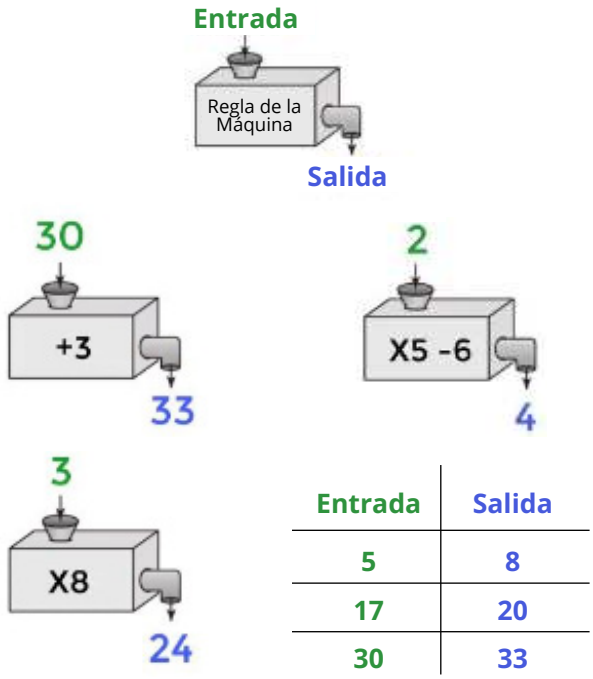
• Si la mayoría, por consenso está de acuerdo que el minero es el ganador, se le da su recompensa.
• Comienzan de nuevo.

○ Si entran más mineros a la próxima competencia, **Bitcoin** reduce el número objetivo de modo que siempre se demore aproximadamente 10 minutos para que alguien gane.

7.2 Un Pequeño Desvío- Para entender la importancia de los hashes

¿Qué es una función?

- Como una máquina transformadora:
  - • Se introduce algo, se modifica median te unas reglas estrictas, y surge otra completamente diferente.
  - • Es decir, se suministra el dato de entrada, *x*, o los datos que uno ingresa.
  - • Se le aplican operaciones matemáticas *(suma, resta, multiplicación, etc.)* predefinidas.
  - - El resultado es una *salida, **f(x),y**.*



Entrada	Salida
5	8
17	20
30	33

- Ejemplo: f(x)=3x+4, me dice:
  - • Multiplique el dato de entrada (x) por 3, súmele 4 y obtenga la *salida* f(x), o y.
  - • ¿Cuál sería la respuesta de f(2)? Es decir, ¿cuál es el resultado de ***y*** cuando ***x***=2?
  - • Ahora, ¿cuál es la pregunta aquí? ***f(x)=15*** ¿Buscamos encontrar la entrada o la salida? ¿Es posible encontrar el valor? Veamos....

f(x)=3x+4=15 ***3x+4=15....*** ***x= ¿?***

- Algunas funciones son *unidireccionales*.
  - • Tienen la propiedad de ser fáciles de calcular pero difíciles de invertir.
  - • Aunque sepamos el *resultado*, no podremos *descifrar* los datos de *entrada*.

- Si odias las matemáticas, vamos a formular una analogía que te ayudará a entender mejor ese concepto.

Vamos a hacer un jugo de frutas rojas.
- • Estos son los datos de *entrada*: *(t=taza)*
- • 1 t agua, 3 cubos de hielo, 18 frambuesas, 8 fresas, 15 t moras y 1/5 de t azúcar.
- • La *operación de la función*:
  - - Lo mezclamos todo junto en la licuadora .
- • Dato de *salida resultado*:
  - - Resulta un jugo delicioso.

• Es casi imposible que otra persona descifre cuales son sus ingredientes y porciones exactas.
• Esto es lo que significa una función unidireccional.
• El jugo no se puede convertir de nuevo en sus datos de entrada.

Los Mineros y la Minería de Bitcoin

¿Qué es un hash?

- **Bitcoin** usa criptografía- una rama de matemáticas.
  - Su proceso de entradas y salidas es muy parecido.
  - Una función *hash* criptográfica:
    - Es una operación criptográfica que toma cualquier cantidad de datos,
    - Devuelve un valor hash, de identificadores *únicos e irrepetibles, determinísticos y caóticos*.

Mi Primer Bitcoin → **Función Hash** → 41798cc97f-682c23159597a-1b039b5abb-9700ff9160b-850dee4d88ad-86bf1594

- No existen restricciones en los datos de entrada:
  - El *hash* siempre resulta en la misma longitud de caracteres.
  - El *hash* también se considera una *huella digital* de los datos de entrada.

GLOSARIO

***Determinístico**: Las mismas entradas o iniciales producirán invariablemente las mismas salidas o resultados.*

***Caótico**: Una entrada ligeramente diferente producirá una salida completamente diferente y no relacionada.*

¿Qué es SHA 256?

- La función hash particular que usa **Bitcoin** se llama *SHA256*.
  - Su *resultado* o *hash* siempre es hexadecimal (números entre 0 y 9 y letras entre A y F).
    - ***SHA256(entrada)=hash***

- Vamos a crear *hashes* Veamos los siguientes ejemplos:

SHA256(Dalia) =
bbadb37bc80b041a1cafdfadf1efd93d
6386117b33046d650e75ec2cb101758c

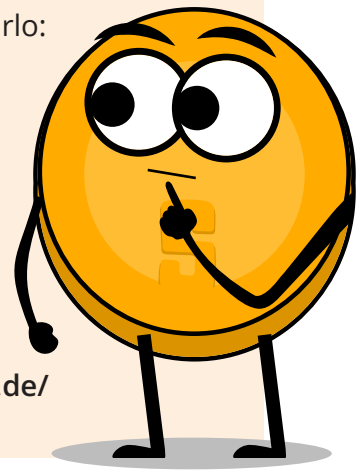
SHA256(DaliaP) =
25cad1ff3deb7bc5ba54ccf1f0fe8e8ff
4a17f58826847b8cae2ddbd6cd6ab77

SHA256(Hola, me llamo Dalia. Soy de Medellín, Colombia.) =
619010e5ab4877ef398e82a277e7134
529a5ff1875f7671ff0177c7ab0302423

Actividad: Creando Hashes

Actividad de Clase. ¿Cómo crear un hash? En los siguientes sitio web podremos practicarlo:

https://hashgenerator.de/



Primero, ¿qué pasa cuando ingresas el hash 256 de *Dalia*, o *Mi Primer Bitcoin*? Compáralo con el que está escrito aquí.

¿Te das cuenta que aunque el resultado es aleatorio?

- El resultado de una entrada en particular siempre será el mismo.

- Si en vez de nombre, apellido y fecha de nacimiento, nos identificáramos con un número así, no habría el problema de tener dos "María" o dos "José" en clase.

¿Cual es el hash de tu nombre? ¿Tu nombre y apellido?

¿Qué pasa si cambias una letra a tu nombre? ¿Hubieras podido predecir este hash?

¿Qué es un "nonce"?

- El término "***nonce***" viene de "number used once".
  - Simplemente es un número usado una vez.
  - Los "***nonce***" son muy útiles para la minería ya que uno de los mayores objetivos es encontrar resultados de los SHA-256(Entrada) que satisfagan ciertas condiciones predeterminadas.

- Supongamos que el **objetivo** es encontrar un hash que **inicie con el número "cero"**.
  - Cambiándole solo el último dígito a SHA(Dalia**P**). El nonce cambiaría la "P" :

SHA(Dalia**1**) = c2cb88c9aec429a7fe9194351e-748247f668241ff75c708b43ea83ecd730268f

SHA(Dalia**2**) = 17df2ae3b1dec56c7bde0cf8b-161f24329d351e08cb797adbd76af46401da-df3

... Estuvimos con suerte y sólo necesitamos intentar ocho veces para lograr nuestro objetivo:

SHA(Dalia**8**)=**0**93d4ddb-855114f49f3b775803529ed1cbd5598b5995c-327091552bab5672658

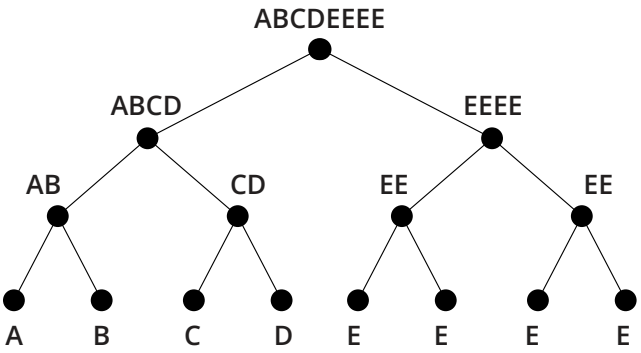
¿Qué es un Árbol de Merkle?

- Una estructura de datos dividida en varias capas de hashes que permite verificar, de forma rápida y eficaz *la información de todas las transacciones*.

- Es como un árbol invertido, en la que se parte desde las hojas y se escala progresivamente a través de las ramas hasta llegar al ***nodo raíz***.

- Que es el identificador principal que permite verificar el conjunto de datos como un todo.

- Su raíz única final, que contiene toda la información de todas las transacciones.
  - Se denomina *Merkle Root*, o *Raíz de Merkle*.



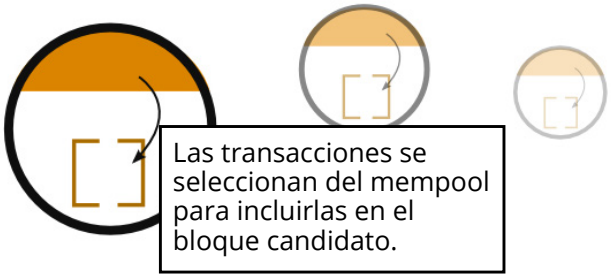
7.3 La Minería

Ahora volvamos al proceso de **Bitcoin**.

- Los mineros tienen libertad de escoger transacciones para incluir en su próximo bloque.
  - Seleccionan y agrupan nuevas transacciones verificadas a un nuevo "bloque candidato".

¿Cuáles transacciones deben escoger para su "bloque candidato"?

- Eligen aquellas con *mayores incentivos monetarios* y que *ocupen menos memoria*.
  - Los depositantes agregan comisiones (o propinas) para incentivar a los mineros.
  - Adicionalmente, los mineros están motivados a trabajar honradamente.



- Entre más transacciones hayan en la mempool, más congestionada la red.
  - Los incentivos monetarios generalmente son mayores cuando hay mucho tráfico.
  - Durante mucho tráfico, los mineros eligen transacciones que tienen comisiones más altas.
  - Una vez el tráfico haya disminuido- se agregan aquellas con menores incentivos.

¿En qué consiste cada bloque candidato?

- El tamaño de un bloque es de aproximadamente 2.5 MB.

- Cada bloque tiene capacidad para unas pocas miles de transacciones como máximo, por lo tanto, es importante elegir eficientemente.
  - Incluye un encabezado de bloque.
    - Este encabezado de bloque se somete a la función hash.

SHA256(*encabezado*) = RESULTADO

¿Para qué se usa este RESULTADO?

- El objetivo es producir un identificador válido para un nuevo bloque, que encaje perfectamente detrás del último bloque en la cadena existente.
  - Para esto, un minero debe producir el "hash ganador".

- El cual será deberá ser por debajo de un "valor objetivo" específico.

• Siempre y cuando el RESULTADO sea mayor que el hash deseado,

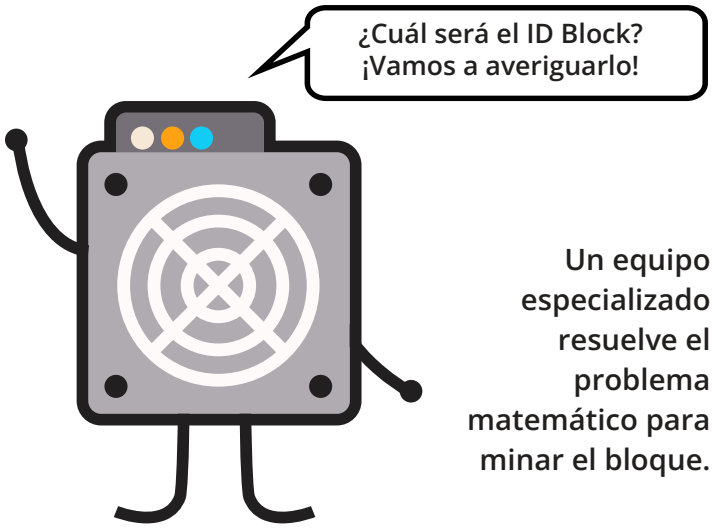
- El minero ajusta un *"nonce"* y vuelve a intentarlo.
- Los mineros repiten esto varios miles de veces por segundo,
- Con la finalidad de ganar la recompensa del bloque.
- Y crear una "huella digital" o un hash único de dicho bloque

• El proceso requiere cambiar el nonce miles y miles de veces, generando muchísimos posibles RESULTADOS, hasta lograr el "hash ganador" antes que cualquier otro minero.

• Muy similar a nuestro ejemplo inicial de lanzar el dado muchas veces, hasta que un minero logra ganar con un RESULTADO debajo de el objetivo.

● Esto significa que cualquier nodo minero en la red puede extraer un nuevo bloque.

• Pero necesita gastar energía para poder hacerlo.



Un equipo especializado resuelve el problema matemático para minar el bloque.

¿Qué pasa cuando se encuentra el "hash ganador"?

● Un minero afortunado, finalmente produce el hash ganador,

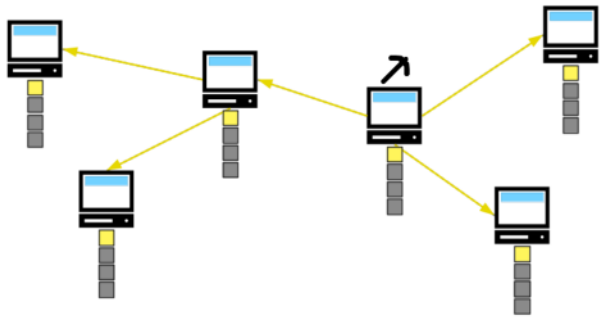
• Transmite su éxito a toda la red.

- Ese *hash* se convierte en el "*hash del bloque*" o su *identificador único*.

● Para el resto de los mineros, la confirmación de la validez del bloque es un proceso simple.

• Sólo se debe asegurar que todas las transacciones sigan siendo validas.

• Y que el hash del bloque sea menor que el "valor objetivo".



● Al ser confirmado el bloque, los otros nodos lo agregarán a la cadena existente.

• Todas las transacciones contenidas en dicho bloque quedarán permanentemente grabadas en la cadena de bloques.

● El proceso se repetirá aproximadamente cada 10 minutos.

• Los mineros comenzarán a intentar extraer un nuevo bloque encima.

¿Y como se gana la recompensa el minero que ha encontrado el valor objetivo?

- Todos los bloques candidatos crean una primera transacción que incluye una recompensa:
  - Contiene una cantidad de ***bitcoin*** nuevo que va a ser liberado cuando se cree el bloque.
    - Y la totalidad de las comisiones que generan las transacciones seleccionadas.

- Solamente el minero ganador puede cobrar dicha recompensa.
  - Por su gran esfuerzo computacional: *PoW, o Prueba de Trabajo*.
    - *PoW* ha sido un método exitoso:
    - Porque encontrar el *hash* es extremadamente difícil, pero verificarlo es muy sencillo.

- A esta transacción se le llama *coinbase*, o *monedabase*.
  - Es la primera en cada bloque de la blockchain.

No Confíes, Verifica

¿Qué quiere decir esto?

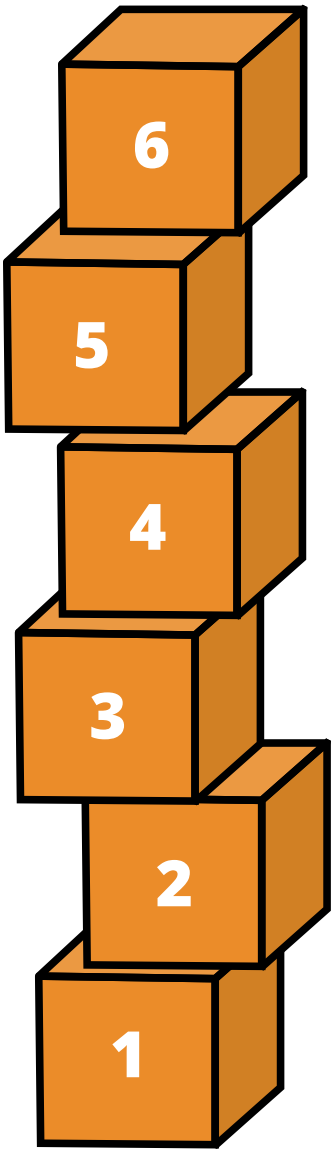
- Las transacciones obtienen una confirmación cuando son incluidas en un bloque y luego tras la confirmación de cada bloque posterior.

- Para que dicho bloque se incluya en la cadena de bloques, se debe enlazar correctamente debajo de el último bloque creado en la red.

- Una confirmación en la blockchain, indica que "la transacción ha sido procesada y validada por la red y es muy poco probable que se revierta".

- Se recomienda esperar un mínimo de seis confirmaciones para asegurarse de que los fondos fueron transferidos.

- Bitcoin es conocida como la blockchain más segura y veraz que existe.



Bloque #6:
6 confirmaciones
Su ransacción es segura.
60 minutos

Bloque #5:
5 confirmaciones
50 minutos

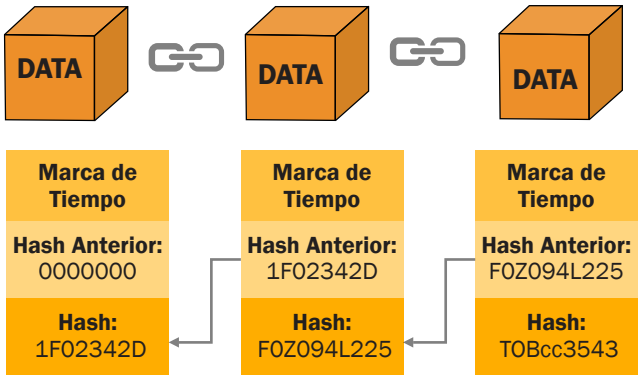
Bloque #4:
4 confirmaciones
40 minutos

Bloque #3:
3 confirmaciones
30 minutos

Bloque #2:
2 confirmaciones
20 minutos

Su transacción está confirmada.
10 minutos

El Hash del Bloque



- Cada bloque hace referencia a un bloque anterior,
  - A través del campo '*bloque anterior*' (*previous hash*) en la *cabecera del bloque*.

- La secuencia de los hashes que unen cada bloque al previo crea una cadena que se remonta hasta el el primer bloque jamás creado.
  - El primer bloque es conocido como el bloque génesis.

- Cualquier modificación mínima a cualquier transacción cambiará el hash del bloque, y lo desligará del bloque anterior.

- Si un hacker trata de alterar hasta una coma de una transacción, se creará una cascada de fallas en la verificación de bloques posteriores.

- Esto se debe a que cada bloque tiene información sobre el anterior.

- Los bloques se componen de una cabecera de bloque y sus transacciones.

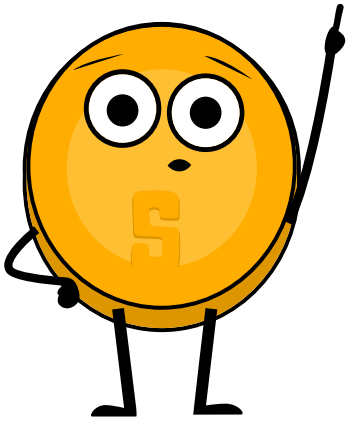
  - El *encabezado* contiene:
  - **1.** El resumen de los datos dentro del bloque, es decir, todas las transacciones comprimidas en una *raíz de Merkle*.
  - **2.** El *hash* del bloque anterior en la blockchain.
  - **3.** Un *nonce*, el cual puede cambiar tantas veces sea necesario en busca de "*valor objetivo*."

- Mediante la función SHA256, se comprime toda la información contenida en el bloque.
  - Este resultado es el "*hash del bloque*" o representant su "*huella digital*".

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c8170100000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

Hash del Bloque

```
0000000000000000
e067a478024addfe
cdc93628978aa52d
91fabd4292982a50
```



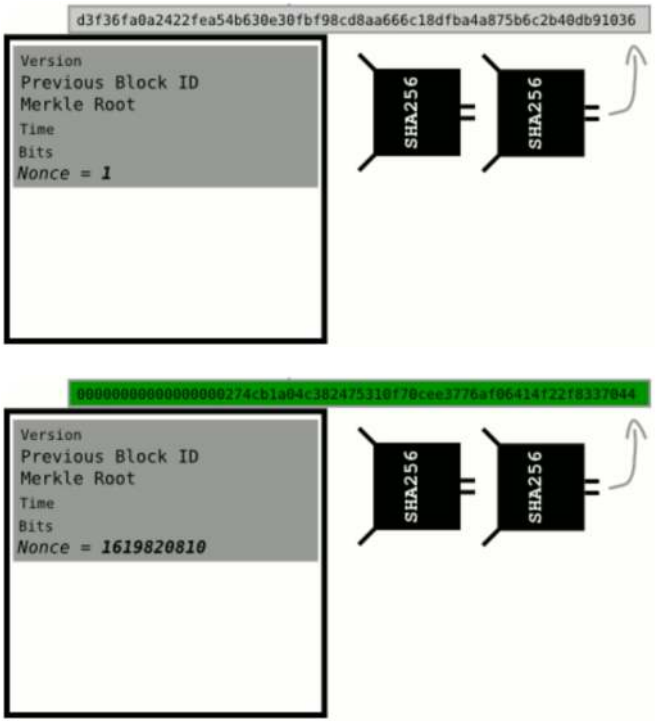
Los Mineros y la Minería de Bitcoin

El Nonce del Bloque

- El *nonce* un campo es un número dentro de la cabecera:
  - Los mineros lo *modifican hasta que* el *hash de la cabecera* resulte en el *objetivo de dificultad o el valor objetivo*.

- El *objetivo de dificultad* siempre comienza con una cantidad de ceros.
  - La cantidad de ceros es variable.
  - Depende cuantos mineros están tratando de extraer el bloque.

- Cuando un minero encuentra un *nonce* que, añadido al hash de cabecera, cumpla el objetivo de dificultad, lo añade a la cabecera del bloque nuevo y lo envía a la red para que el resto de mineros puedan comprobar que la solución es válida.



Actividad: Analizar Bloques en Tiempo Real

Actividad de Clase. En el siguiente enlace se puede analizar la cadena de bloques en tiempo real. Responde las preguntas en base a la información del sitio web.

1. ¿Cual fue el último bloque minado?

2. ¿Cuántas transacciones se incluyeron en dicho bloque?

3. ¿Cuál es el valor total transado en bitcoin?

4. ¿Cuánto fue el tamaño en MB del bloque?

5. ¿Con cuántos ceros comienza el *nonce* del bloque?

6. ¿Cuanto ganó el minero en total?

7. ¿Cual fue el valor total de las comisiones que recibió el minero por adicionar las transacciones a la red?

8. Escoge una de las transacciones de más valor del bloque. ¿La cantidad de BTC se repartió a cuantos monederos?

Clase #8

La Escasez, el Costo, el Precio y la Volatilidad

8.1 La Importancia de la Recompensa del Bloque
8.2 Halving
- Eventos de Reducción a la Mitad

8.3 El Valor de Bitcoin a través del Tiempo
- Factores a Mediano y Largo Plazo
- El Efecto Lindy

8.4 Las Recompensas a los Mineros
- La Dificultad

8.5 ¿De qué o de quién me tengo que cuidar?
- Los ataques a Bitcoin
- ¿Qué es un ataque del 51%?

La Escasez, el Costo, el Precio y la Volatilidad

8.1 La Importancia de la Recompensa del Bloque

Para crear un sistema económico descentralizado exitoso:

- Los mineros invierten dinero y trabajo computacional para minar ***bitcoins***.

- Aseguran la red para evitar ataques, y al mismo tiempo:
  - Generan monedas nuevas que pueden circular libremente en la red.

- La recompensa por bloque actúa como un subsidio e incentivo para los mineros.
  - Las tarifas o las comisiones de transacción garantizan que no existan fallos en la red.

8.2 Halving

- Satoshi Nakamoto diseñó una forma muy estratégica de distribuir nuevos ***bitcoin*** sin que una persona o un grupo de personas estuviera encargada de repartirlos.

- Con el fin de perseguir un modelo deflacionario se estableció que:
  - Cada 210.000 bloques se reduce el número de ***bitcoin*** liberados a la mitad.
    - Esto sucede aproximadamente cada cuatro años.
  - A diferencia de los problemas a los que nos enfrentamos con las monedas fiat, donde nadie sabe realmente cuánto crédito o dólares hay en el sistema,
    - **Bitcoin** tiene una oferta total fija de 21.000.000.
    - Este tope fijo de suministro se controla de forma automatizada.
    - Se hace cumplir a través del consenso.
  - Al inicio, la recompensa se fijó en 50 ***bitcoins*** por bloque.
  - Aproximadamente cada cuatro años, la recompensa se reduce a la mitad, por lo que se denomina evento de *halving*.

Eventos de Reducción a la Mitad

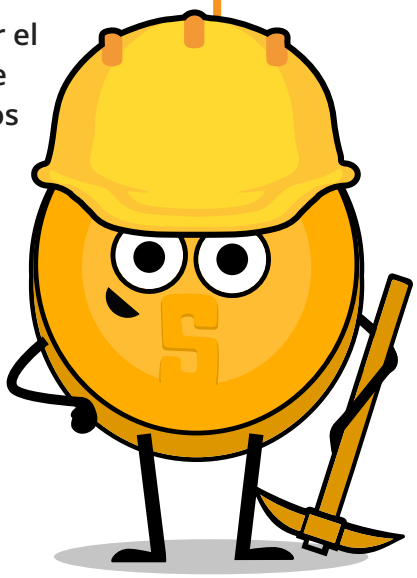
- El primer *halving* se produjo a finales de 2012.
  - El bloque 210,001 sólo otorgó 25 BTC.

- El segundo evento ocurrió en 2016.
  - La recompensa se redujo a 12.5 BTC.

- Y así seguirá hasta el año 2140.
  - Cuando se habrán extraído los 21 millones de ***bitcoins***.

- Esta reducción a la mitad de las recompensas se ha añadido con la intención de:
  - Prevenir la inflación
  - Añadir escasez natural

Aquí puedes ver el número total de bitcoins minados que circulan actualmente en la red.



Entonces, ¿por qué el cambio? ¿Por qué no mantener la recompensa igual? ¿No es eso injusto para los mineros?

La respuesta a esa pregunta está en la ley de la oferta y la demanda.

- Si las monedas se crean demasiado rápido y no hay límite para la cantidad de ***bitcoin*** que se pueden crear:
  - Pronto habrá demasiados ***bitcoin*** en circulación y su valor disminuirá.

- Si los 21 millones se hubieran liberado a la vez:
  - Es posible que unas pocas personas lo hayan acaparado.
  - Nadie más hubiera tenido la oportunidad para acumularlo.

- El siguiente gráfico ejemplifica cómo la reducción a la mitad afecta el precio a lo largo del tiempo:

8.3 El Valor de Bitcoin a través del Tiempo

El valor de ***bitcoin*** ha aumentado:

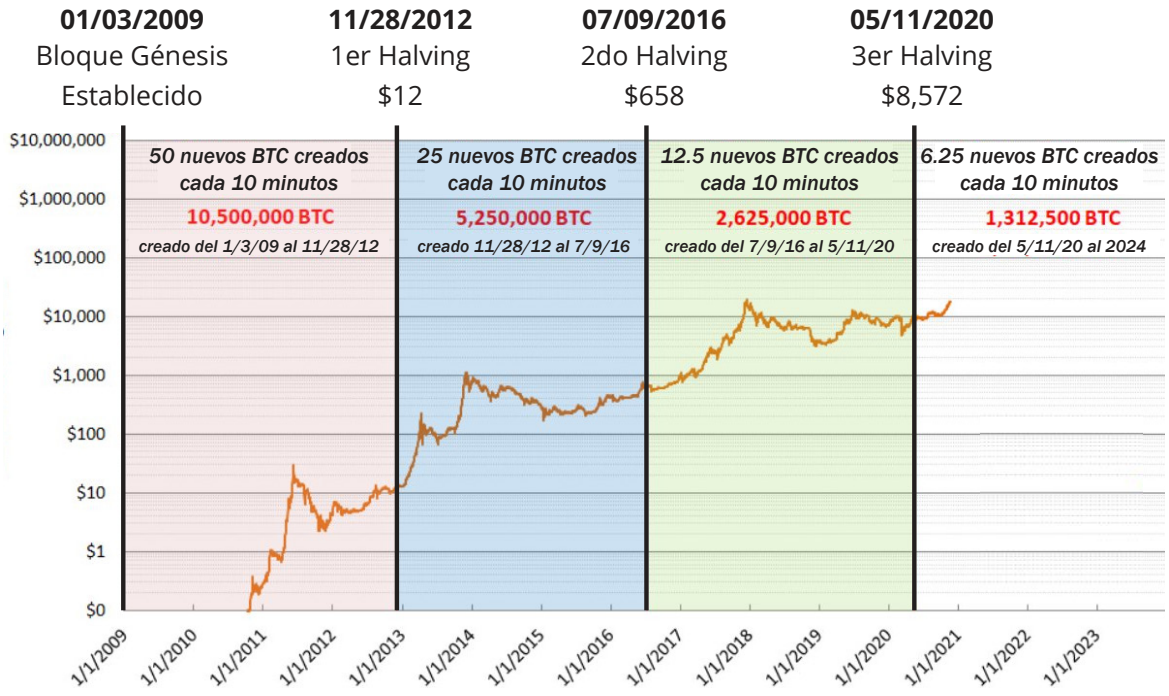
- De menos de $0.01 en el 2009 (en primera transacción).

- Hasta un máximo de alrededor de $67,000 USD, en noviembre de 2021.

- En la última década, aunque ha tenido caídas de hasta 80%, no sólo se ha recuperado, sino que a largo plazo, su tendencia es a la alza.

- Los factores que afectan la oferta y demanda se han diversificado

  - *¿Por qué es valioso bitcoin?*
  - *¿Por qué ha subido tanto el precio?*
  - *¿Por qué es tan volátil?*



La Escasez, el Costo, el Precio y la Volatilidad

Para entender mejor esto, hay algunos términos importantes que debemos definir:

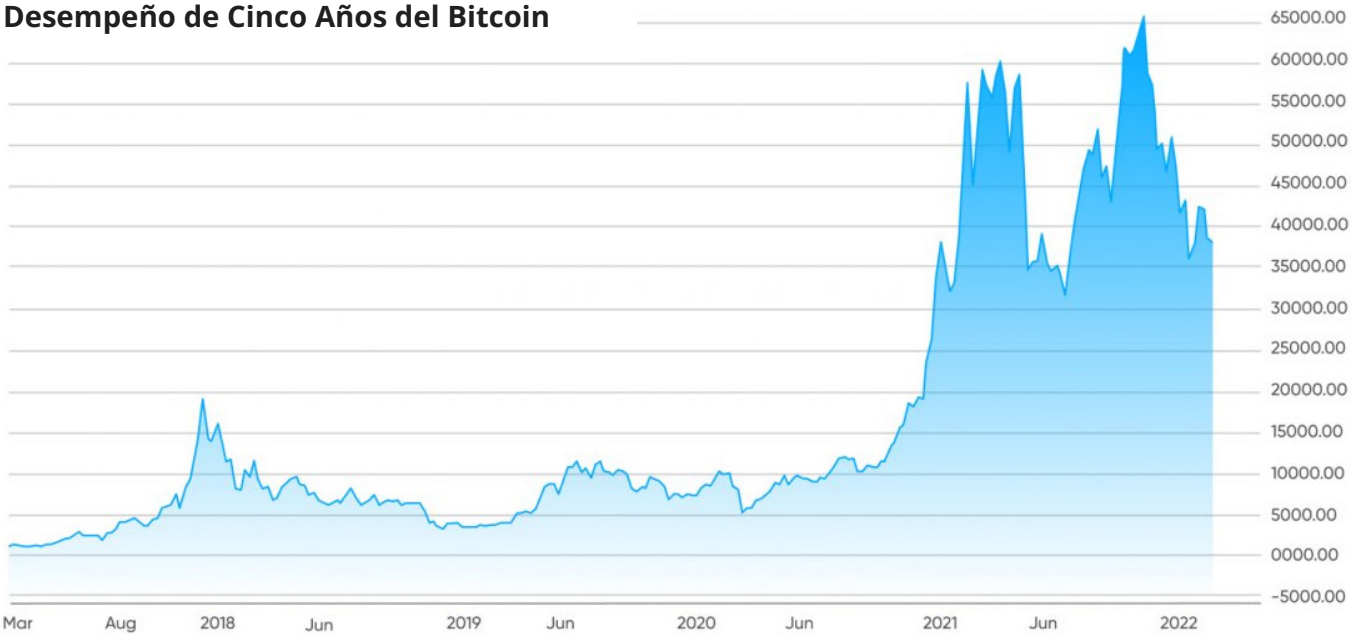
- **1. Suministro Circulante:**
  - La cantidad de ***bitcoin*** creados hasta el momento.
  - Hasta julio del 2022, se han creado aproximadamente 19,101,000 ***bitcoin***.

- **2. Suministro Total:**
  - Cantidad de monedas ya en circulación, más monedas que no han sido extraídas.
  - En total, el suministro total de ***bitcoin*** será de 21 millones.
    - Se estima que faltan o se consideran "perdidos" alrededor de 4 millones de ***bitcoin***.
    - Se cree que no se pueden gastar debido a contraseñas perdidas, direcciones de salida incorrectas o errores en el programa.

- **3. Capitalización de Mercado:**
  - El valor de mercado total del suministro circulante de ***bitcoin*** reflejado en *monedas fiat*.
  - Multiplicar el precio actual de un ***bitcoin*** (en USD) por la oferta circulante.

Capitalización de Mercado =
Precio Actual x Suministro Circulante

Desempeño de Cinco Años del Bitcoin



- El gráfico de la página anterior, vemos el precio de ***bitcoin*** en los últimos 5 años.
  - Esta es una manera fácil de visualizar qué tan sensible o volátil es el precio.
    - El eje **X** es para el tiempo y el eje **Y** es para el precio en USD.

¿Qué eventos mundiales podrían relacionarse con los cambios de precios?

Entonces, ¿qué factores determinan su precio? ¿Cómo se involucra la minería? ¿Cuándo afecta el halving al precio?

- La demanda sigue permanentemente creciendo.

- Su sistema de suministro de oferta es fijo.

- Es un activo naciente de sólo 13 años de vida el cual apenas empieza a ser regulado.
  - Por supuesto que se espera volatilidad en su precio.
  - No obstante, su precio ha tenido al alza desde su creación.

Analiza el gráfico histórico de los precios de bitcoin.

ColinTalksCrypto.com

Factores a Mediano y Largo Plazo

- Los factores que determinan el precio de ***bitcoin*** se pueden analizar a mediano y largo plazo. A continuación veremos cada uno de ellos.

Factores a Mediano Plazo:

- *Comercio Diario*
  - A diferencia de otros mercados financieros, opera 24 horas al día, los 7 días de la semana.
  - Las transacciones se pueden realizar por medio de dispositivos móviles.
    - Permite intercambiar fácilmente cualquier cantidad de ***bitcoin***.
  - Para *HODLERS* esto es una pesadilla, ya que el precio puede cambiar hasta un 20% en un solo día.
  - Para *traders*, es una oportunidad para aprovechar estos cambios de precios y obtener ganancias.

- *Noticias y Eventos Mundiales*
  - Sensible a eventos mundiales, noticias y especulaciones.

- *Costos de Minería*
  - Los mineros son los responsables de agregar más y más bitcoin al suministro total.
  - Si los costos de electricidad suben, los mineros se ven obligados vender entre el 40%-60% de sus ***bitcoin***, ya que deben cubrir las facturas y los gastos de hardware.

- *Burbujas de Mercado*
  - En los últimos años, los compradores de ***bitcoins*** son cada vez más diversos y sus hábitos de compra y ahorro varían.
  - El tamaño de su participación en **Bitcoin** y su comportamiento hacia él pue de cambiar el precio general de ***bitcoin***.

- *Regulaciones Gubernamentales*
  - A diario aumenta la normativa de las

criptomonedas, esto puede afectar el valor de ***bitcoin***.
- Joe Biden presentó una ley en la cual, a partir de ahora, las transacciones de activos digitales por valor de más de 10.000 dólares se deben declarar al *Servicio de Impuestos Internos.*

Factores a Largo Plazo:

• *Halving*
- La recompensa de bitcoin pasa a ser la mitad alrededor de cada 4 años.
- La recompensa de los mineros disminuye drásticamente en esos momentos.

• *Adopción Masiva*
- Si todo el mundo lo comienza a usar, un proceso denominado *hiperbitcoinización*, y por extensión, invierte más de su dinero en ***bitcoin***, el precio subirá exponencialmente.

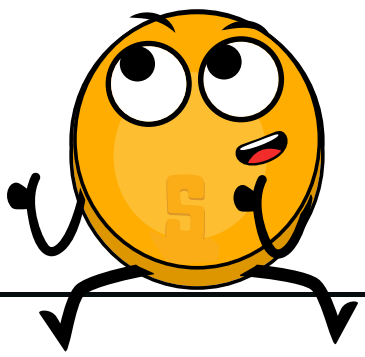
1998 2005 2014 2021

2012 2013 2014 2021

• *El Efecto Lindy*
- Es una teoría sobre el envejecimiento de las cosas no perecederas.
  - Cuanto más antigua sea una idea o una tecnología, mayor será su esperanza de vida.
- Las cosas no perecederas como la tecnología envejecen, linealmente, a la inversa.

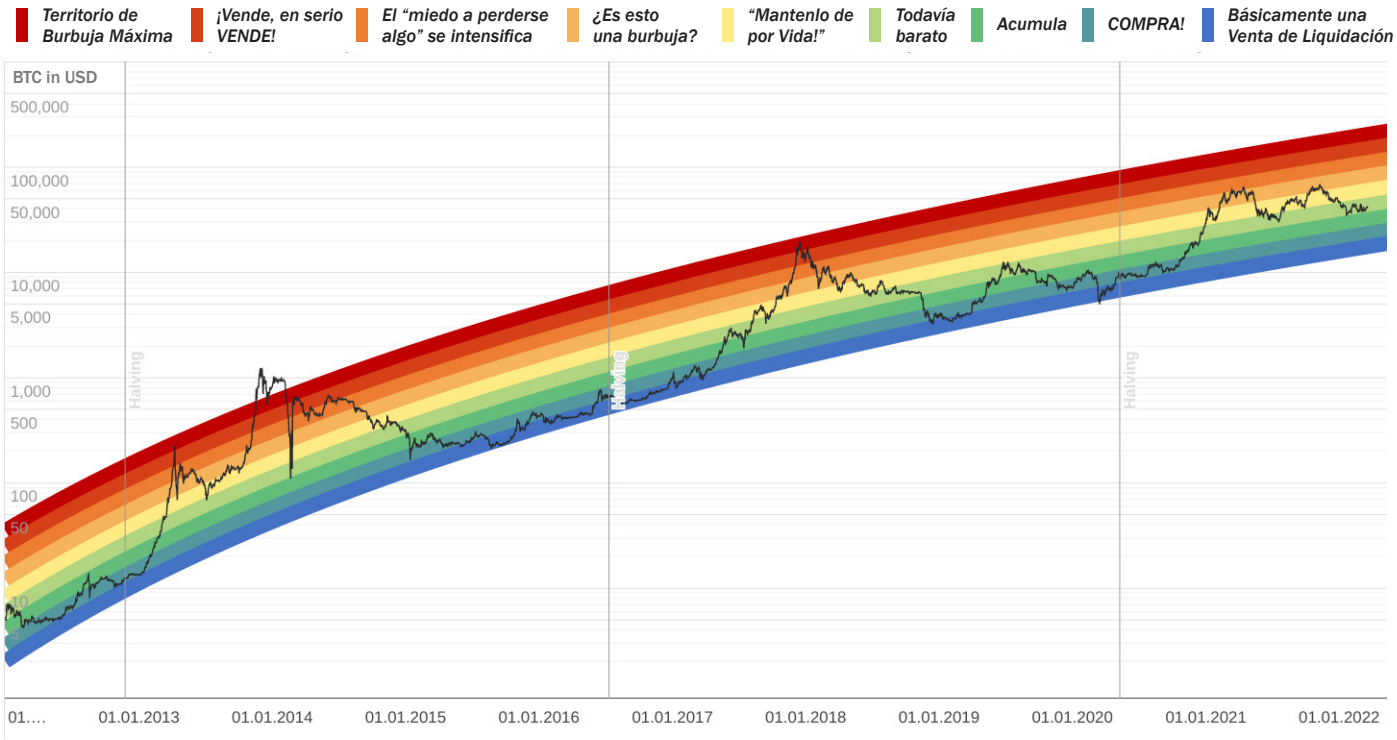
• *Oferta Limitada*
- El hecho de que solo haya una cantidad finita de ***bitcoin*** significa que no es posible diluir el sistema después de 2140.

- El "*gráfico arcoíris*" usa una escala logarítmica para visualizar el precio de ***bitcoin***.
  ○ La división de colores:
    - Muestra cuándo la moneda está sobrevendida (zonas azul y verde).
    - O cuándo está sobrecomprada (zonas naranja, roja y morada).
  ○ *Este gráfico nos da* información valiosa para determinar estrategias de compra y venta de ***bitcoin***.
  ○ Algunos inversionistas muy exitosos esperan pacientemente:
    - Compran cuando el precio llegue a la zona azul/verde.
    - Venden poco a poco, mientras el precio se acerca a la banda roja.



Gráfica de El Efecto Lindy

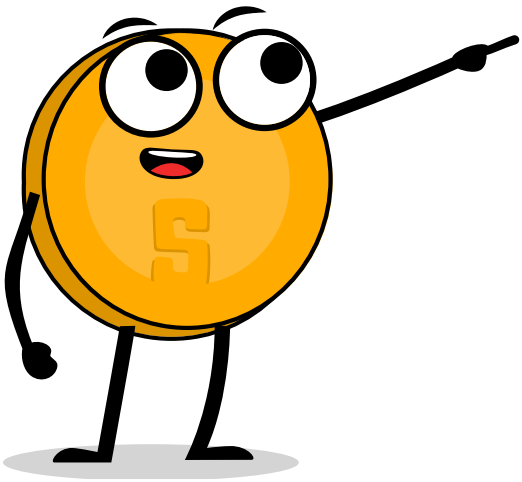
Gráfico Arcoíris



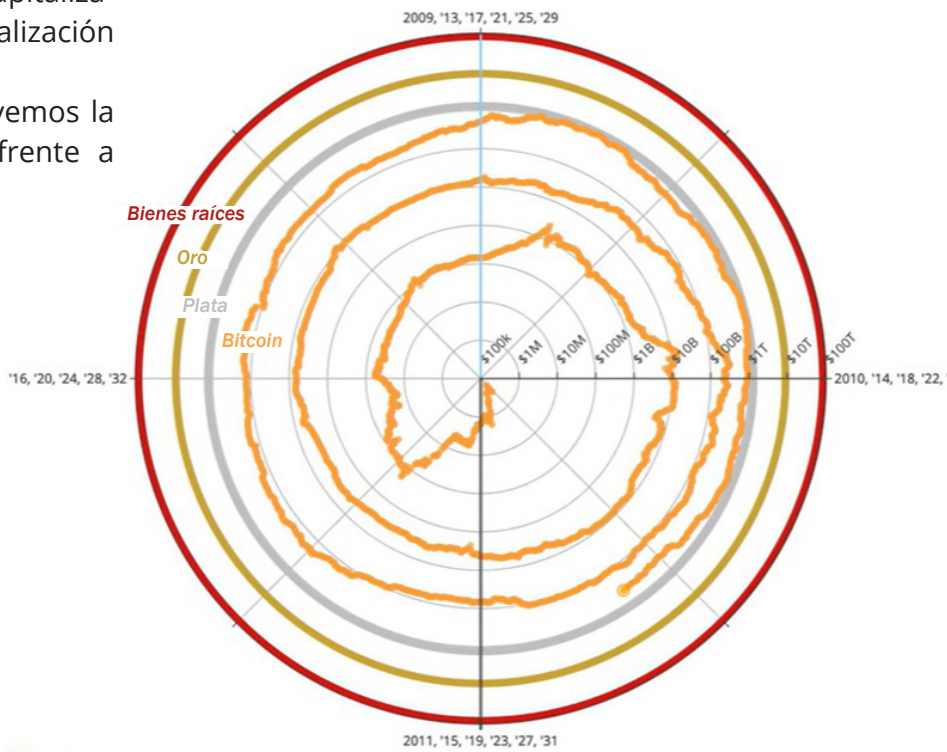
La Escasez, el Costo, el Precio y la Volatilidad

● Veamos en perspectiva, y a través de ciclos de cuatro años, el crecimiento en la capitalización de ***bitcoin*** en relación con la capitalización de otros activos monetarios globales.

- En la gráfica de la derecha, vemos la capitalización de mercado **Bitcoin** frente a oro, plata y bienes raíces.



Espiral de Activos Cruzados



8.4 Las Recompensas a los Mineros

● Veamos como han cambiado las recompensas y los incentivos monetarios a los mineros a través del tiempo y observamos que existen épocas más rentables que otras.

• El incentivo de los mineros aún permanece, independientemente de las recompensas más pequeñas, ya que el valor de ***bitcoin*** aumenta a largo plazo en el proceso.

Ingresos Totales de Mineros
$34,688,409.61

La Dificultad

● La dificultad es una medida de lo trabajoso que es extraer un bloque de **Bitcoin**.

• O de encontrar un hash por debajo del "valor objetivo" propuesto.

● La dificultad se ajusta cada 2016 bloques (*cada 2 semanas aproximadamente*).

• Para que el tiempo medio entre cada bloque se mantenga en 10 minutos.

● El ajuste de la dificultad está directamente relacionado con la *potencia minera total*.

• Se estima en terahashes/segundo (TH/s). (Tera = trillón)

- La red de hoy tiene la capacidad de calcular trillones de hashes por segundo.

- Entre más alta la dificultad, más poder de cómputo para minar la misma cantidad de bloques, lo que hace que la red sea más segura contra los ataques.

8.5 ¿De qué o de quién me tengo que cuidar?

Aunque **Bitcoin** puede ofrecer mucha mayor protección que el sistema financiero tradicional, las estafas de dinero a las víctimas desprevenidas cada vez es más sofisticado. Como por ejemplo:

- Suplantación de Identidad.
  - El atacante puede obligar al destinatario a revelar información sensible
    - Roba sus credenciales después de inducirlo a cambiar la contraseña.
    - Roba sus claves privadas y por lo tanto su bitcoin.
    - Lo induce a visitar un sitio web con malware y toma control sobre su computadora.
- Secuestros de DNS o de extensiones de navegador
  - Los atacantes secuestran sitios web legítimos.
    - Los sustituyen por interfaces fraudulentos.
    - Engañan a los usuarios para que introduzcan sus **claves privadas** en estos sitios falsos.
- Un hacker puede intercambiar las tarjetas SIM de dos móviles y robar todos los datos.
  - Los ciberdelincuentes buscan sacar provecho de cualquier situación. Las empresas y los equipos de seguridad están luchando para mantenerse al día.

Los ataques a Bitcoin

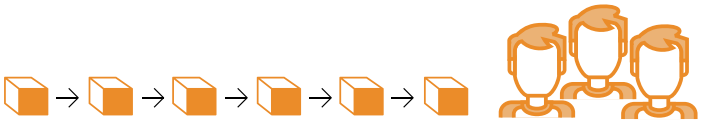
Los ataques físicos que se conocen a Bitcoin.

- Ninguno de estos ataques ha podido lograr interrumpir la red de **Bitcoin**.
- Si las **claves privadas** permanecen en un lugar seguro.
  - Los atracos se vuelven prácticamente imposibles.
- De todos modos, existe la pequeñita posibilidad de un ataque del 51%.

La Escasez, el Costo, el Precio y la Volatilidad

¿ Qué es un ataque del 51%?

- Para lograrlo, se necesitaría trabajo, energía y centralización de computación.

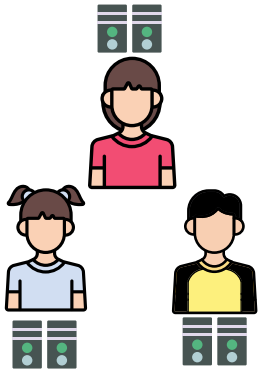


La mayoría de los mineros están agregando y transmitiendo bloques a la cadena de bloques pública.

Un atacante está agregando bloques a una cadena de bloques privada y no los transmite a la cadena de bloques pública.

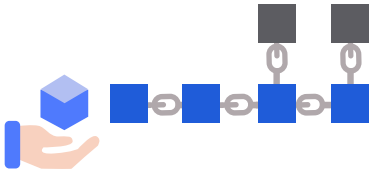
- Un minero malicioso tendría que acumular más del 50% del poder computacional de la red.
  - La red *ya no sería descentralizada*, sino controlada y manipulada por dicho minero.
  - Se crea una cadena nueva atada a la cadena original.
    - Esto terminaría engañando a algunos de los participantes para que adicionen sus bloques ella.
    - Puede fácilmente *manipular*, *alterar* o *desencadenar* la cadena a su beneficio.
    - Puede robar dinero a través del doble gasto y/o censurando transacciones.

- Este tipo de ataque nunca ha sucedido con **Bitcoin**.



En las redes basadas en PoW existen múltiples participantes (nodos mineros) que agregan nuevos bloques y confirman la información en la cadena de bloques.

Los mineros compiten entre sí para ganar el derecho a que su versión de un nuevo bloque sea confirmada por la mayoría de los participantes.



Clase #9

Bitcoin de Hoy y del Futuro

9.1 La Energía Consumida
9.2 Innovación
- Software- Bitcoin Core
- SegWit, Taproot, y Firmas Schnorr
- Taro

9.3 Bitcoin y el futuro de El Salvador

Bitcoin de Hoy y del Futuro

9.1 La Energía Consumida

¿Bitcoin realmente consume tanta energía como se cree?

Para aumentar las ganancias:

- Los mineros conectan una gran cantidad de computadores.
  - Con el objetivo de aumentar sus posibilidades de conseguir ***bitcoin***.

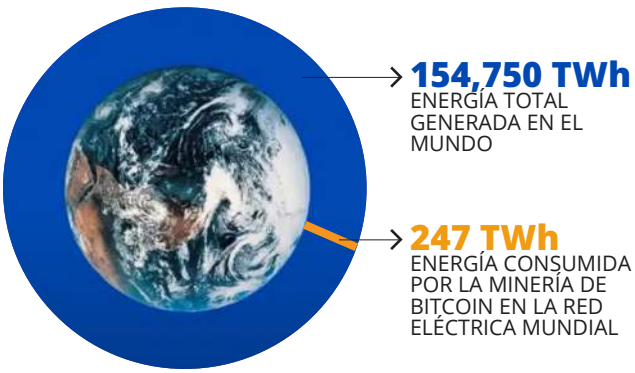
- Los computadores trabajan casi día y noche para ganarse las "loterías",
  - Por lo tanto, el consumo eléctrico es considerablemente alto.

- La tecnología que se usa para la minería de **Bitcoin** se está volviendo cada día más limpia,
  - Tanto que la adopción de energías sostenibles subió al 59,5% en abril 2022.

- Aunque el hash rate de **Bitcoin** ha crecido un 23% comparado con principios del 2021
  - El consumo eléctrico de la minería de BTC es un 25% menor al de aquel entonces.

- Los ASIC actuales son 100 mil millones de veces más veloces que los CPU's del 2009.

- La energía consumida por **Bitcoin** representa un 0.16% de la energía a nivel mundial.

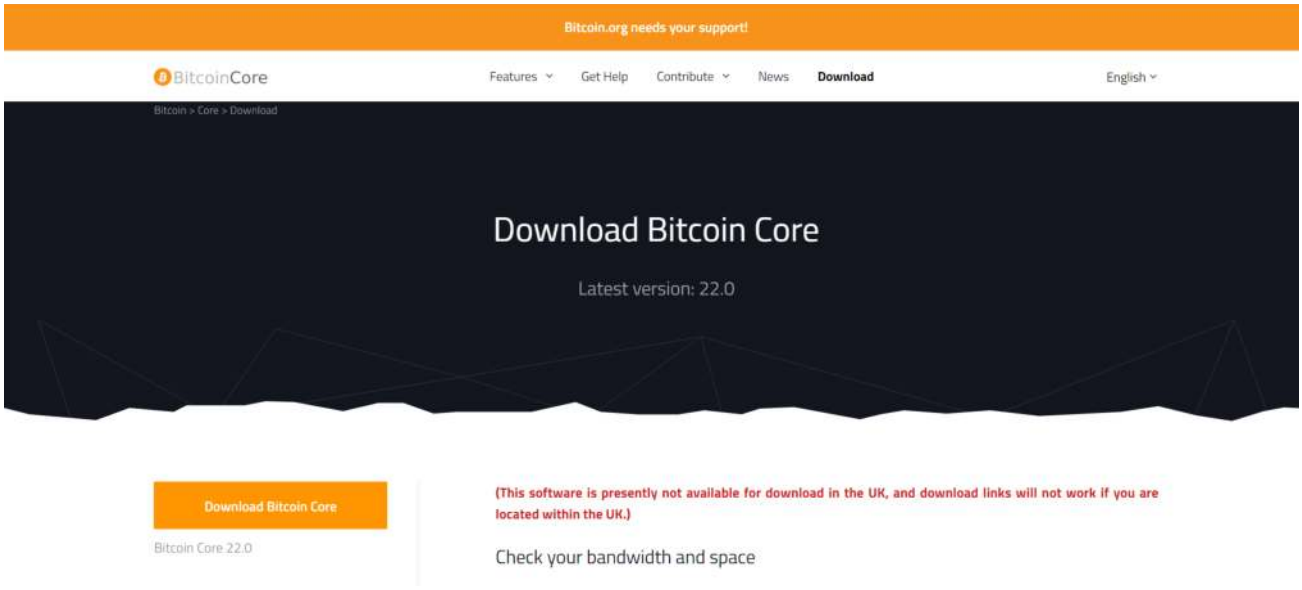


9.2 Innovación

Software- Bitcoin Core

- Bitcoin Core es el software original creado por Satoshi Nakamoto.
  - Diseñado para conectarse a otras personas que ejecutan el mismo programa,
    - Creando una red de computadoras que se comunican entre sí.
  - Su propósito es que al descargarlo, todos trabajen con el mismo conjunto de reglas.
    - Para validar transacciones.
    - Y contribuir con la seguridad y la descentralización del sistema.
  - Quien lo ejecute, puede instalarlo como cualquier otro programa.
    - Descarga y crea una copia adicional de la cadena entera de bloques.
    - Puede ayudar a transmitir transacciones a otras computadoras.
  - Siempre y cuando haya acceso a inter net, no se necesita ningún permiso para:
    - Descargarlo y/o utilizarlo con toda libertad.
    - Transferir ***bitcoin*** a otro monedero o recibir de alguien más.
    - Verificar de forma demostrable la emisión de la oferta.
    - Conocer el historial de transacciones y los propietarios de cada ***bitcoin***.

- Decenas de expertos en software y criptografía, trabajan en su mantenimiento y mejora.
  - Quien propone una actualización en el software, requiere el consenso de la mayoría de los para implementarla.



Código Fuente Abierto

Cualquier persona puede ver, proponer cambios, modificar y distribuir como mejor le parezca. Es comparable a ir a un restaurante y tener acceso a las recetas de tus comidas favoritas (el código)... pero luego puedes hacerlas y agregar o quitar cualquier ingrediente que desees y perfeccionarlas.

SegWit, Taproot, y Firmas Schnorr

Bitcoin ha mejorado a través del consenso, a través de Propuestas de Mejoras de Bitcoin, BIP's. Esto lo ha vuelto más seguro y eficiente con los años.

- Primero, ***SegWit***, un soft fork que se implementó en el 2017,
  - Aumentó el límite de tamaño de los bloques eliminando partes de las transacciones.
  - Mejoró la velocidad de procesamiento de las transacciones de Bitcoin.
  - Arregló un punto débil del protocolo que permitía a los nodos:
    - Manipular los problemas de maleabilidad de las transacciones (TXID) en la red.
    - La ***maleabilidad*** de una transacción es cuando un atacante puede modificar o alterar el hash de una transacción dentro del blockchain.

- Segundo, ***Taproot*** se creó para mejorar la privacidad y aumentar el anonimato en la red.
  - Taproot, puede "*camuflar*" transacciones.
  - Reduce los tiempos de validación de las transacciones.
    - Lo cual podría ayudar a fomentar a bitcoin como medio de pago.
  - Las comisiones de las transacciones se podrían reducir de manera notable.

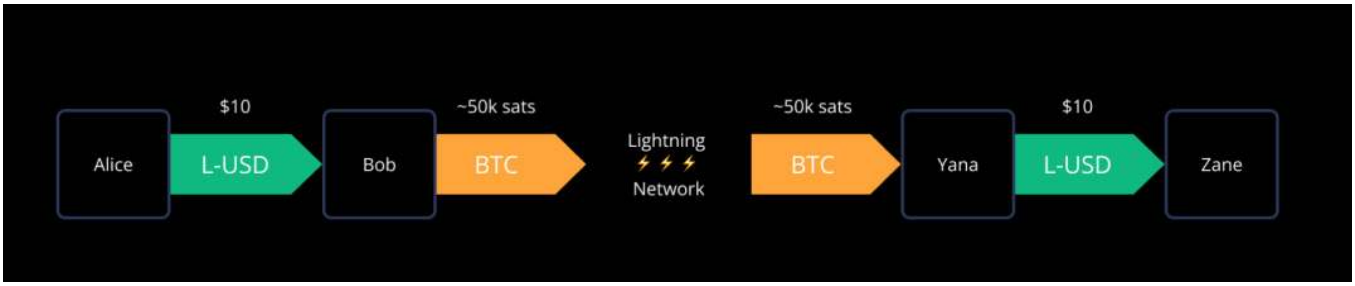
- La sustitución a firmas ***Schnorr***; reemplaza la actual *firma digital de curva elíptica* (ECDSA).
  - Integra varias claves dentro de una transacción compleja y generar una firma única.
  - Simplifica los contratos inteligentes en la blockchain.
  - Ayuda a escalar los canales de pago de segunda capa, como la ***Lightning Network***.

Taro

- Con el nuevo protocolo ***Taro*** se aspira llevar la tecnología **Bitcoin** a otro nivel.

- Permitirá la emisión de monedas estables y otros activos en la red Lightning.

- Se podrá intercambiar cualquier divisa por otra instantáneamente, prácticamente gratis.



9.3 Bitcoin y el futuro de El Salvador

- La originalidad y las posibilidades de **Bitcoin** ha captado la atención de:
  - El mundo de la inversión
  - El mundo corporativo.
    - Tanto las empresas públicas como las privadas están sujetas a los mismos impactos de la inflación y supresión de intereses a los los ahorradores.
    - Buscan reforzar sus balances.
    - Poseen grandes reservas de efectivo.
    - Están adaptando bitcoin como reserva de valor a largo plazo.

- Es probable que El Salvador tenga una ventaja gigante frente al mundo en un futuro.
  - Se ha convertido en el primer país en hacer Bitcoin moneda de curso legal, en paralelo con el dólar estadounidense.
    - Bitcoin Beach ya es un proyecto robusto y sólido. Ha lograd crear una economía circular dentro de una comunidad costera.

  - El FMI y el Banco Mundial se han pronunciado en contra de esta decisión.
    - Mientras tanto, El Salvador sigue acumulando satoshis.

- ¿Quién será el próximo en hacer Bitcoin moneda de curso legal?
  - Los países que fomenten la adopción cuanto antes, probablemente se beneficiarán más.

- El dólar estadounidense parece estar al borde del colapso, con el rublo (Rusia) y el yuan

(China) tomando un papel más importante en la geopolítica.

- Ambas son monedas fiduciarias, compitiendo contra ***bitcoin***.

- Varios países están tratando de implementar *monedas digitales del banco central* (CBDC):
  - Intentos de crear monedas fiduciarias con beneficios digitales.
  - Implica que el gobierno puede vigilar cada transacción.

¿Quién está comprando Bitcoin?

- Rusia está dispuesta a aceptar petróleo y gas en ***bitcoin***.
- Rio De Janiero está dispuesto a aceptar impuestos inmobiliarios en ***bitcoin***.
- Algunas ciudades de EE. UU. están dispuestas a aceptar impuestos en ***bitcoin***,
- Algunos funcionarios gubernamentales en EE.UU aceptan sus salarios en ***bitcoin***.

- Bitcoin en el futuro:
  - Permitirá innovar masivamente en soluciones de Capa 2.
  - Modernizará contratos, activos y credenciales en el ámbito privado y público.
  - Alentará a los países a cooperar en lugar de competir.
  - Cesará el deseo de manipular las economías mediante la impresión de dinero.
  - Incluso puede ser que los países y estados-nación ya no existan, y algo nuevo los remplace, con la ayuda de **Bitcoin**... ¿quién sabe?

"Tanto si crees que puedes hacerlo, como si no, en los dos casos tienes razón."

- Henry Ford

Actividad de Clase. Responde las siguientes preguntas según lo que has aprendido en las últimas clases.

¿Cuáles crees que son los beneficios más importantes de **Bitcoin**?

¿Qué imaginas que podría pasar en El Salvador en los próximos diez años?

¿Crees que los salvadoreños se familiarizarán más con **Bitcoin** y lo encontrarán una tecnología esencial?

9.4 Actividad: Simulador de Bitcoin

Actividad de Clase. Sigue las siguientes instrucciones:

Crear una nueva billetera.

Ya hemos creado una llamada ***MiPrimerBitcoin***.

La **clave privada** es:
e17a9fe1f9cade3f1f8b6426f9fdabe27d0378d931fc8bb5bbb1d25d7c33e6e5

La cual ha minado 2 bloques (2830, 2831) y ha hecho una transacción.

Por lo tanto, lo que puedes hacer ahora:

1. Minar un bloque para recibir tu primer bitcoin como recompensa.
2. Firmar transacciones y enviar ***bitcoin*** a otras billeteras.
3. Crear tu propia cadena de bloques privada y usar el simulador con grupos no públicos o clases escolares.
4. Crear transacciones falsas con un nombre falso e intentar obtener ***bitcoin*** mediante fraude.
5. Realizar un ataque del 51% para manipular posteriormente la cadena de bloques.
6. Contárselo a otras personas.

¡Cuanto más entiendas cómo funciona Bitcoin, mejor!

Clase #10

Proyecto Final

- ¿Por qué Bitcoin?

Proyecto Final

¿Por qué Bitcoin?

Ejercicio Práctico. Escriba un ensayo argumentativo de una a dos páginas y asegúrese de cubrir todos los siguientes puntos:

- Explica qué es **Bitcoin**.
- Explica cómo funciona **Bitcoin**.
- En su opinión, ¿Cuáles son al menos dos formas en que **Bitcoin** cambia la forma en que opera el mundo hoy? Justifique su respuesta.

Clase Adicional

La Magia de las Firmas Digitales

- Claves Públicas y Privadas
- La Firma Digital
- Transacciones Válidas

La Magia de las Firmas Digitales

Claves Públicas y Privadas

Ahora que entendemos los retos de seguridad, volvamos a los monederos y las transacciones.

La mayoría de los monederos más seguros proporcionan:

- Una "**clave privada *maestra***" o una "*semilla*"
  - Es una lista generada por el monedero aleatoriamente de 12 a 24 palabras.
    - Nadie más en el mundo ha visto jamás.
    - Es la clave única que permite acceder al ***bitcoin*** del usuario en cualquier dispositivo.
    - Se usa para como génesis para crear cada una de las **claves privadas**.

- Cada **clave privada** genera una **clave pública**.
- Cada **clave pública** nos permite *firmar* digitalmente una *transacción*.
- Cada *transacción* tiene una **firma digital** única.
- Cada **firma** permite transferir ***bitcoin*** a una *dirección* en particular.

Entremos en detalle:

- Private Key = Clave Privada
- Public Key = Clave Pública
- Address = Dirección
- Generate = Generar

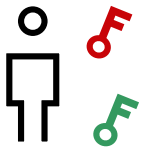
- **Clave Privada**:
  - Comparable con una contraseña y debe mantenerse a salvo de cualquier tercero.
  - En caso perder el monedero, es una forma de recuperar el ***bitcoin***.
  - A menos que se tengamos una "*semilla*"
    - Las claves privadas son números completamente aleatorios y grandísimo entre 1 y 1157920892373161954235709850086879078528375642790749043826051631415181614943 36.
  - Cualquier clave privada se convierte a una estructura hexadecimal:
    - Un número de 0-9, A-F, donde A=10, B=11, etc.
  - Es prácticamente imposible generar la misma clave privada dos veces.

Practica generar una llave privada en el siguiente enlace.

Learn Me a Bitcoin

- **Clave Pública**:
  - Usando la **clave privada** como dato de entrada,
    - Se usa una multiplicación matemática muy avanzada para generar la clave publica.
  - La operación es unidireccional- no se puede reversar.

Ejemplo de Clave Privada



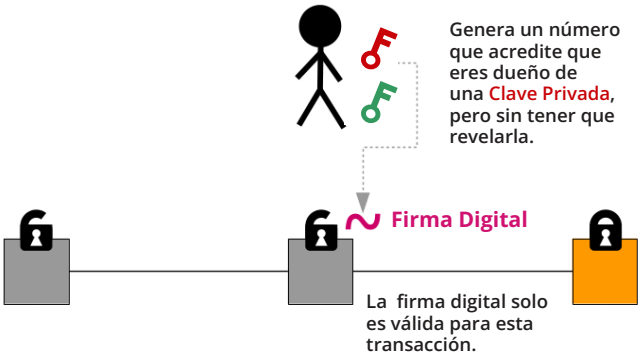
458717487902476942636812561412180509625
405580735281576561171132573666848711 18

28165556693891620773477477574559423752 7
92107203189219630880988688806282470022 5

La Clave Pública se calcula a partir de la Clave Privada

La Firma Digital

- Se usa para demostrar que conocemos la clave privada sin revelarla públicamente.
- Se calcula a partir de la clave privada y de la información incluida en la transacción,
- Es única, irrepetible e imposible de falsificar.
- Es obligatoria para desbloquear el ***bitcoin*** que el emisor va a trasladar.



Detengámonos un momento...

Si un hacker intercepta tu transacción, ¿crees que sea capaz de descifrar tu clave privada y robarte tus fondos? Es decir, suponiendo que una persona maliciosa tenga acceso a la dirección a la cual vas a enviar bitcoin, ¿crees que puede redirigirlo a su propia caja de seguridad?

Transacciones Válidas

El objetivo de una firma digital es poder demostrar que se es propietario de una clave pública.

- Los mineros verifican la firma con la clave pública del emisor.
- La verificación criptográfica es similar a:
  - Evidenciar que la última pieza en un rompecabezas encaje correctamente.
  - Si la transacción se modifica en lo más mínimo.
  - El hash de la firma automáticamente cambia, haciéndola falsa y obsoleta.
  - Es extremadamente fácil detectar las transacciones que se deben rechazar.

Fuentes

1. The Free Silver Movement, Scott Wolla, Federal Reserve Bank of St. Louis. https://www.stlouisfed.org/-/media/project/frbstl/stlouisfed/education/lessons/pdf/the-free-silver-movement-and-inflation.pdf,

2. Video - ¿Qué es el Dinero? MagicMarkers. TV, Colombia. https://youtu.be/2yCIKkq8gKA

3. https://www.philadelphiafed.org/-/media/frbp/assets/institutional/education/lesson-plans/functions-and-characteristics-of-money-lesson.pdf, Functions and Characteristics of Money, Chapter 3, Segment 301, Federal Reserve Bank of Philadelphia

4. https://www.philadelphiafed.org/-/media/frbp/assets/institutional/education/lesson-plans/money-grades-6-8.pdf, "Why Money", Bonnie T. Meszaros, Federal Reserve Bank of Philadelphia

5. https://www.kansascityfed.org/documents/2856/teachingresources-Lessonplangr9-12.pdf Federal Reserve Bank of Kansas

6. ¡Historia de 1870 a 1971 en 10 minutos!, Robert Breedlove. Para la sección de 1870-1914: https://www.forbes.com/sites/nathanlewis/2013/01/03/the-1870-1914-gold-standard-the-most-perfect-one-ever-created/?sh=5e0ab9864a6a

7. Economía Desde Cero: Dinero-Video, https://youtu.be/zcYw8a4RJC4, Canal Encuentro, Argentina.

8. https://www.kansascityfed.org/documents/2856/teachingresources-Lessonplangr9-12.pdf, Activity 5, Auction, Federal Reserve Bank of Kansas.

9. Video - Qué es la Inflación, https://youtu.be/gkDQGribCfc](https://youtu.be/gkDQGribCfc, Banco de la República de Colombia

10. Video - ¿Cómo Nos Vigilan en Internet?, Magic Markers https://youtu.be/-sWgOuFIaws](https://youtu.be/-sWgOuFIaws,

11 McDonalds Menú Picture 1973. https://muddyrivernews.com/opinion/daily-dirt-where-were-you-in-72-or-once-upon-a-time-when-a-big-mac-was-65-cents/20220323091958/

12. McDonalds Menú 2022. McDonalds El Salvador, Twitter.

13. Causas de la Inflación, Video, Banco de la República, Colombia.

14. Declining purchasing power of the US dollar strengthens Bitcoin, https://cryptopotato.com/is-there-a-pattern-between-usd-dow-jones-and-bitcoin/, Toju Ometoruwa.

15. Ejemplo de Estado de Cuentas, https://www.ejemplode.com/59-finanzas/4274-ejemplo_de_estado_de_cuenta.html

16. Video - MagicMarkers.TV,Colombia. ¿Qué es Bitcoin y Cómo Funciona?, https://youtu.be/S2HxMK7iO4c,

17. Nodos Completos - Visualización de una Transacción http://beautifuldata.net/2015/01/querying-the-bitcoin-blockchain-with-r/

18. Video - (https://youtu.be/lD8WQbS8-T8), *Que es La Red Relámpago*, Whiteboard Crypto en Español

19. Bitcoin en Números, Nick Carter, Bitcoin Demystified.

20. Bitcoin, Will the Price of Bitcoin Rise or Fall?, Capital.com Research Team, 08:00 (UTC), 31 March 2022. https://capital.com/de/bitcoin-prognose,

21. U.S. dollar inflation visualized at the top versus bitcoin's deflation at the bottom: Lark Davis @TheCryptoLark.

22. https://www.bitcoincharts.com

23. https://www.blockchaincenter.net/en/bitcoin-rainbow-chart/

24. https://www.blockchain.com/charts/miners-revenue


Mi
Primer
Bitcoin
EL SALVADOR