El LIBRO DE bitcoin MÁS SIMPLE JAMÁS ESCRITO

Keysa Luna

* Dar la pastilla Naranja: * to orange-pill: (verb) / tu' ȯr-inj-'pil/
: Explicar Bitcoin de manera que un pre-coiner lo entienda, ¡y se convierta en Bitcoiner!

1 bitcoin = 100,000,000 satoshis

El Libro de Bitcoin más Simple Jamás Escrito

Portada y diseño interior por Keysa Luna
Imagen de portada por Vallota de pixabay.com
Traducción al español por Ôkami: Twitter: @_Okami9
Edición de la versión en español por: Monika Bravo Twitter: @BravoMonika
Publicado de forma independiente

TABLA DE CONTENIDO

Para todos nuestros niños

Agradecimientos a Satoshi y a los cypherpunks

Me encanta la vida sencilla,
Me encanta la naturaleza, me encanta estar descalza,
me encantan las conversaciones profundas que
despiertan la creatividad,
conexión, e inspiración.
Me encanta la libertad.

Y me encanta Bitcoin.

Amor es una gran palabra, y Bitcoin es digno de un gran amor.

Su existencia es un punto de luz brillante en este momento tan desafiante de la existencia humana.

Escribí este libro con la esperanza de hacer que Bitcoin, y las razones por las cuales lo necesitamos, sean más accesibles para aquellos que buscan conocerlo!

¡Este libro es un punto de partida hacia lo que yo, y muchos otros, hemos descubierto que es una madriguera de conejo infinita, hermosa y capaz de cambiarte la vida!

¡Toma la pastilla naranja, sé libre, y que este viaje te enriquezca!

NOTA: ¡Todo lo expuesto en este pequeño libro está sujeto a debate, discusión, actualizaciones y correcciones!

Como todo en la vida, existen numerosos puntos de vista sobre el bitcoin, su futuro y cualquier otro aspecto del mismo.

En Twitter se pueden encontrar comentarios, tanto confusos como clarificadores, las 24 horas del día, 7 días a la semana. Y es, sin embargo, un recurso inestimable (hasta que una plataforma mejor y descentralizada obtenga una amplia adopción) para interactuar con personas que han estado muy metidas en la madriguera de conejo, durante mucho tiempo…

Todo este ecosistema es un proceso emergente, popular, desordenado y fascinante. Se trata, con diferencia, del mayor experimento a nivel mundial jamás emprendido, con personas de todas las razas, religiones, clases y creencias que se comprometen juntas y sin problemas a descubrir una nueva forma de avanzar.

¡Si te inspira este movimiento, es muy probable que caigas en la madriguera de conejo con el resto de nosotros!

Por las mentes y corazones abiertos en el camino…

Recuerda: No confíes, Verifica.

¡Y siempre busca más información por tu cuenta!

He desarrollado un nuevo sistema de dinero electrónico P2P [de igual a igual] de código abierto llamado Bitcoin. Es completamente descentralizado, sin servidor central ni partes de confianza, porque todo se basa en la prueba criptográfica en lugar de la confianza. Pruébalo, o echa un vistazo a las capturas de pantalla y al documento de diseño.

Descarga Bitcoin v.0.1 en:
http://www.bitcoin.org

~ Satoshi Nakamoto, 11-9-2009, 22:27:00 UTC
Publicado en metzdown.com, una de las primeras listas de correo criptográfico

POR QUÉ NECESITAMOS bitcoin

NECESITAMOS bitcoin
PORQUE EL DINERO ESTÁ PERDIDO

La raíz del problema con la moneda convencional es toda la confianza que se requiere para que funcione. Se debe confiar en que el banco central no degrade la moneda, pero el historial de las monedas fiduciarias está lleno de violaciones de esa confianza. Los bancos deben ser confiables para guardar nuestro dinero y transferirlo electrónicamente, pero lo prestan en burbujas de crédito con apenas una fracción de reserva. Tenemos que confiar en ellos para nuestra privacidad, confiar en que no permitan que los ladrones de identidad limpien nuestras cuentas.

~ Satoshi Nakamoto 2009-02-11

- El sistema monetario como tal está roto, no funciona bien (siempre lo ha estado)
- Es insostenible (nunca lo ha sido)
- No hay forma de arreglarlo (nunca la habrá)

EL (NO) PATRON DEL ORO

- La mayoría de la gente cree que el dinero está respaldado por el oro.
- No lo está.
- No lo ha estado desde 1971, cuando el Presidente Nixon sacó al mundo del patrón oro de manera unilateral (el shock de Nixon).
- Mira wtfhappenedin1971.com para tener una idea más clara del daño que causó esto.

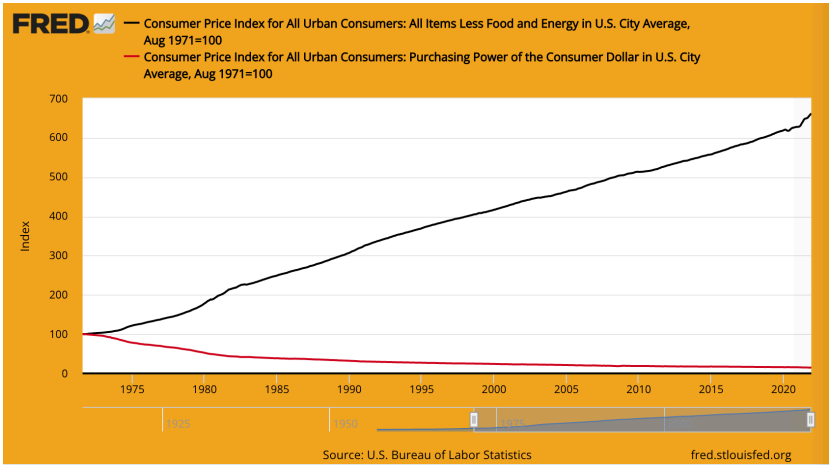


Gráfico que muestra la inflación del IPC (línea negra) frente al poder adquisitivo del dólar (línea roja) desde 1971.

➢ **Dato Curioso:** El Foro Económico Mundial [WEF] se creó en 1971.

FIAT: (noun) /ˈfiːˌæt/
: una orden autorizada o arbitraria **:** DECRETO
: una determinación autorizada **:** DICTAMEN
: una orden o acto de voluntad que crea algo sin o como si sin más esfuerzo
~ merriam-webster.com/dictionary - Google translate

FIAT : del Latin fieri "*fiat*, 'hágase"

- El dinero Fiat sólo tiene valor porque el gobierno dice que lo tiene.
- Por lo tanto, la gente cree que es así (está obligada a hacerlo)
- **Aún si no lo creen, por ley están forzados a usarlo, y a aceptarlo como pago por bienes y servicios.**
- **El dinero Fiat es creado de la nada.**
- Actualmente, el 3% de los dólares se imprime como efectivo.
- El 97% restante es creado por bancos introduciendo cifras en un ordenador (¡no es broma!) cuando emiten préstamos.

A la Oficina de Grabado e Impresión le cuesta sólo unos centavos producir un billete de 100 dólares…

~ Barry Eichengreen, Economista Americano

Scott Pelley de '60 Minutes', NBC: *¿Es justo decir que simplemente inundaron el sistema con dinero?*
Jerome Powell, Presidente de la Reserva Federal: *Sí. Lo hicimos. Esa es otra forma de pensarlo. Lo hicimos.*
Pelley: *¿Y de dónde sale?*
¿Lo imprimen sin más?
Powell: *Lo imprimimos digitalmente. Como Banco Central, tenemos la capacidad de crear dinero digitalmente. Y lo hacemos comprando Letras del Tesoro o bonos por otros valores garantizados por el gobierno. Y verdaderamente, eso aumenta la oferta monetaria. También imprimimos moneda como tal, y la distribuimos a través de los bancos de la Reserva Federal.*

~ Entrevista de '60 Minutes' de la CNBC, 17 de mayo de 2020.
Dos meses tras el inicio del confinamiento por el C*vid19

Realmente no hay límite para lo que podemos hacer con los programas de préstamos que tenemos.

~ Jerome Powell, Presidente de la Reserva Federal

Sí, existe una cantidad infinita de efectivo en la Reserva Federal. Haremos lo que sea necesario para asegurarnos de que haya suficiente efectivo en el sistema bancario.

~ Neel Kashkari, Presidente de la Reserva Federal de Mineápolis

El "nosotros", aquí se trata de cinco personas que votan sobre cambios en la política monetaria dentro del sistema de la Reserva Federal durante las reuniones del Comité de Operaciones del Mercado Abierto. 5 de 330.000.000. Esto es todo lo que se necesita para cambiar la política monetaria de EE.UU.

~ @MartyBent, Fundador de TFTC.io

CITAS NOTABLES

El banco obtiene su beneficio del interés del dinero que crea de la nada.

~ William Paterson, 1694,
Fundador del Banco de Inglaterra

Todas y cada una de las dudas, confusiones y angustias en América surgen, no de los defectos de la Constitución o Confederación, no de la falta de honor o virtud, sino de la total ignorancia de la naturaleza de la moneda, el crédito y la ***circulación.***

~ John Adams
2º Presidente de los Estados Unidos,1735–1826

Creo que las instituciones bancarias son más peligrosas para nuestras libertades que los ejércitos permanentes. Ya han levantado una aristocracia del dinero que ha desafiado al gobierno. El poder de emisión debe ser arrebatado a los bancos y restituido a aquellas personas a quien les pertenece realmente.

~ Thomas Jefferson
3er Presidente de los Estados Unidos, 1801-1809

Mientras nos jactábamos de nuestras nobles acciones, tuvimos cuidado de ocultar el feo hecho de que, por un sistema monetario inicuo, hemos nacionalizado un sistema de opresión que, aunque es más refinado, no es menos cruel que el antiguo sistema de esclavitud.

~Horace Greeley (1811-1872)
Congresista estadounidense y Fundador de The New York Tribune.

Quien controla el volumen de dinero en cualquier país, es dueño absoluto de toda la industria y el comercio…cuando te das cuenta de que todo el sistema es controlado muy fácilmente de una forma u otra por unos pocos hombres poderosos que están en la cima, no será necesario que te digan cómo se originan los períodos de inflación y depresión.

~ James A. Garfield, 20° Presidente de los Estados Unidos de América, Mar-Sept. 1881, Asesinado en 1881

A día de hoy existe, sin control y en manos de un grupo de hombres, el poder de hacer dólares de la nada.

~ Thomas W. Lawson, Frenzied Finance, 1905

Yo era tan reservado -tan furtivo, de hecho- como cualquier conspirador. Sabíamos que el descubrimiento simplemente no debía suceder, o de lo contrario, todo nuestro tiempo y esfuerzo se desperdiciarían. Si se descubriera que nuestro grupo en particular se reunió y redactó un proyecto de ley bancario, dicho proyecto de ley no tendría ninguna posibilidad de ser aprobado por el Congreso.

~ Frank A.Vanderlip
Presidente del National City Bank de Nueva York (precursor del Citi Bank)
~ Escrito de 1935 sobre la reunión secreta que tuvo lugar en Jekyll Island en 1910, para redactar el proyecto de ley que se aprobó como Ley de la Reserva Federal en 1913.

Esta Ley (de la Reserva Federal) establece el acto de confianza más gigantesco del mundo. Cuando el Presidente (Woodrow Wilson) firme el Proyecto de Ley, se legalizará el gobierno invisible del Poder Monetario…El peor crimen legislativo de todos los tiempos, lo perpetra este Proyecto de Ley Bancario y Monetario.

~ Charles A. Lindbergh, Sr. (1859-1924)

Soy un hombre muy infeliz. He arruinado sin querer a mi país. Una gran nación industrial está controlada por su sistema de crédito. Nuestro sistema de crédito está concentrado. El crecimiento de la nación, por tanto, y todas nuestras actividades, están en manos de unos pocos hombres. Nos hemos convertido en uno de los peores y más controlados y dominados gobiernos en el mundo civilizado. Ya no somos un gobierno por la libre opinión, la convicción y el voto de la mayoría, sino un gobierno por la opinión y la coacción de un pequeño grupo de hombres poderosos.

~ Woodrow Wilson,
28° Presidente de los Estados Unidos,
1913-1921, 6 años después de aprobar la Ley
de la Reserva Federal de 1913.

La verdadera naturaleza del asunto es, como usted y yo sabemos, que un elemento financiero en los centros más grandes *ha sido el dueño del gobierno desde los días de Andrew Jackson.*

~ Franklin D. Roosevelt, 32° Presidente de los Estados Unidos, en una carta escrita el 21 de Noviembre de 1933 al Coronel E. Mandell House

[La depresión] no fue accidental. Fue un hecho cuidadosamente ideado…Los banqueros internacionales trataron de generar un estado de desesperación aquí con el fin de poder emerger como gobernantes de todos nosotros.

~ Congresista Louis T. Mcfadden (Asesinado en 1936)
Presidente del Comité de Banca y Moneda

Cada vez que un banco hace un préstamo, se crea un nuevo crédito bancario, nuevos depósitos, nuevo dinero.

~ Graham F.Towers,
Gobernador del Banco Central
de Canadá, 1934-55

Si no hubiera deudas en nuestro sistema monetario, no habría dinero.

~ Marriner Eccles, 1941, Gobernador de la Reserva Federal

Todavía no he tenido a nadie que pueda, mediante el uso de la lógica y la razón, justificar que el gobierno Federal tome prestado el uso de su propio dinero… Creo que llegará el momento en que la gente exigirá que esto se cambie. Creo que llegará el momento en que este país en el que realmente nos culparán a usted, a mí y a todos los demás relacionados con el Congreso por permanecer de brazos cruzados y permitir que un sistema tan absurdo perdure.

~Wright Patman, Congresista Demócrata, 1928-1976. Presidente del Comité de Banca y Moneda, 1963-1975

Cuando usted o yo emitimos un cheque, debe haber fondos suficientes en nuestra cuenta para cubrir el cheque, pero cuando la Reserva Federal emite un cheque, no existe un depósito bancario sobre el cual se gire ese cheque. Cuando la Reserva Federal emite un cheque, está creando dinero.

~ Banco de la Reserva Federal de Boston, "Putting It Simply", 1984

LA RESERVA FEDERAL

- La Reserva Federal (FED en inglés) es el banco central "independiente" de EE.UU. Fue creado en 1913 con la aprobación de la Ley de la Reserva Federal.
- **Tiene una estructura única, en parte privada y en parte gubernamental.**
- Se supone que es una entidad políticamente independiente y no partidista dentro del gobierno.
- Si bien la Junta de Gobernadores de la Reserva Federal es nombrada por el Presidente y confirmada por el Congreso, **las decisiones de la Reserva Federal no necesitan ser aprobadas por nadie. ¡Sí, es algo confuso!**

Consta de:

- La Junta de Gobernadores de la Reserva Federal
- 12 bancos de la Reserva Federal
- El Comité de Operaciones de Mercado Abierto (FOMC en inglés), que es el organismo que elabora la política monetaria.

La Reserva Federal es responsable de:

- Supervisar la política monetaria de EE.UU., promover el empleo y la estabilidad de los precios.
- Regular y supervisar las instituciones bancarias y financieras.
- Prestación de servicios de pago a entidades financieras.
- Promover la protección del consumidor y el desarrollo de la comunidad.

UN APUNTE SOBRE LA PRESIDENCIA DE LA RESERVA FEDERAL

El presidente también se encarga de:

- Presidir el Comité de Operaciones de Mercado Abierto (FOMC), el cual decide la dirección de la política monetaria en EE.UU. (por ejemplo: Flexibilización Cuantitativa (QE en inglés), subidas de tipos de interés)
- Es miembro del Fondo Monetario Internacional (FMI)
- Es miembro del Banco de Pagos Internacionales (BIS en inglés) (el banco de los bancos centrales).
- Es el ministro de finanzas del G-7
- Es el ministro de finanzas del G-20

¡Mucho poder para una sola persona!

BANCA DE RESERVA FRACCIONAL, INTERESES Y PRÉSTAMOS

- **Banca de Reserva Fraccionaria:** hasta Marzo de 2020, los bancos debían mantener una reserva del 10% de sus activos y podían prestar el 90%.

- **Desde Marzo de 2020, no se requiere una reserva, lo que permite a los bancos emitir préstamos ilimitados (¡¡¡!!!)**

- Un préstamo es dinero basado en deuda, y se deben pagar intereses sobre dicho préstamo.

- **Dato Curioso 1:** El dinero para pagar los intereses del préstamo NO lo crean los bancos.

- **Dato Curioso 2:** NUNCA se crea.

- **Dato Curioso 3:** NO HAY SUFICIENTE dinero préstamos + los intereses adeudados por dichos préstamos.

- **Dato Curioso 4** ¡Nunca lo habrá!

UN APUNTE SOBRE EL PETRODÓLAR

- Se podría decir que, **hasta 1971, el dólar estuvo respaldado por el oro y, desde 1974, ha estado respaldado por el petróleo y, de facto, por el ejército estadounidense.**

- **En 1974, EE.UU. y Arabia Saudí llegaron a acuerdos bilaterales para fijar el precio de la venta de petróleo en dólares estadounidenses.**

- Desde entonces, la mayoría de las ventas mundiales de petróleo se han liquidado en dólares estadounidenses.

- Esto ha contribuido en gran medida a que el dólar se convierta en la moneda más fuerte del mundo.

- **Por tanto, se ha propulsado artificialmente,** incluso en los momentos en que normalmente le hubiera costado más.

- Mientras he estado escribiendo esto, las cosas se han deteriorado rápidamente. A medida que se intensificaba la invasión rusa de Ucrania, y Rusia y China estaban haciendo tratos por el petróleo en rublo/yuan, rompiendo con el uso del dólar.

- Es muy probable que este pueda ser el principio del fin del petrodólar. Lo que sucederá a continuación está aún por ver…

SOBRE LA FLEXIBILIZACIÓN CUANTITATIVA (QE)

- La Flexibilización Cuantitativa se considera una "política monetaria no convencional" utilizada por los Bancos Centrales para "estimular la economía", mediante la cual la Reserva Federal compra bonos del gobierno y otros valores de éste.
- Fue utilizada por primera vez en Japón entre 2001 y 2006. Después de eso, EE.UU., Reino Unido y la Eurozona usaron Flexibilización Cuantitativa o QE durante la crisis financiera de 2008.
- Desde entonces, la única vez que EE.UU. no ha tenido un programa de QE fue entre 2014 y 2019.
- Como se ve a continuación, los críticos sostienen que la Flexibilización Cuantitativa beneficia de forma abrumadora a quienes ya son ricos.

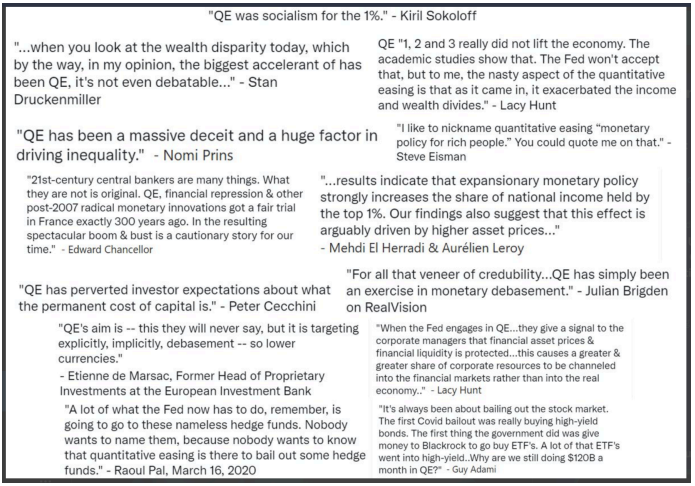


Imagen (Créditos: @RudyHavenstein en Twitter

CICLOS

- **En toda naturaleza hay ciclos, corrientes, expansiones y contracciones.**
- **Esto contribuye a un equilibrio y sostenibilidad general** a lo largo del tiempo, de todo un sistema interconectado de toda vida en la Tierra.
- **El sistema de dinero fiat basado en la deuda ignora la sabiduría de los ciclos naturales** y, en cambio, se basa y depende al 100% de un crecimiento sin precedentes y sin paliativos para su supervivencia, a fin de continuar pagando sus deudas.
- En la naturaleza, esto es un cáncer.
- En "la economía" esta trayectoria antinatural se ve respaldada por parte del gobierno, con el rescate de los bancos y las grandes empresas en quiebra, en lugar de permitirles quebrar y ser "reciclados" en algo nuevo y más sano
- **El cortoplacismo de rescatar empresas en quiebra está poniendo en riesgo a toda la economía.** En esencia, es darle patadas a una lata, y es probable que la agitación que se avecina sea mucho más intensa que si se permitiera que los acontecimientos se desarrollasen como un ciclo de la naturaleza.
- **Estamos en deuda con Satoshi Nakamoto, y con los cypherpunks de antes y después de él;** por tener la visión, previsión, determinación y habilidad para proporcionarnos un bote salvavidas que nos lleve a nuevas costas.

- Una vez nos demos cuenta del regalo que esto supone, depende de nosotros subir a bordo, de todo corazón y con la mente clara, emprender el viaje y construir un nuevo mundo con el Dinero de la Paz.

- **Bitcoin se ocupa de arreglar el dinero, de nosotros depende arreglar el resto. Y, para ser claros, al arreglar el tema del dinero, se arreglarán, por extensión, MUCHAS otras cosas.**

- La principal es que las guerras a gran escala, iniciadas por los gobiernos, ya no serán rentables ni posibles sin el apoyo del pueblo.

- Además, de forma natural habrá menos consumo, ello, junto a un cambio hacia bienes y servicios de valor real, mercados libres, ahorros reales y desmonetización de las viviendas y **bienes raíces,** que en primer lugar, nunca tuvieron la intención de monetizarse.

NECESITAMOS ₿ bitcoin
PORQUE LA INFLACIÓN ES UN ROBO

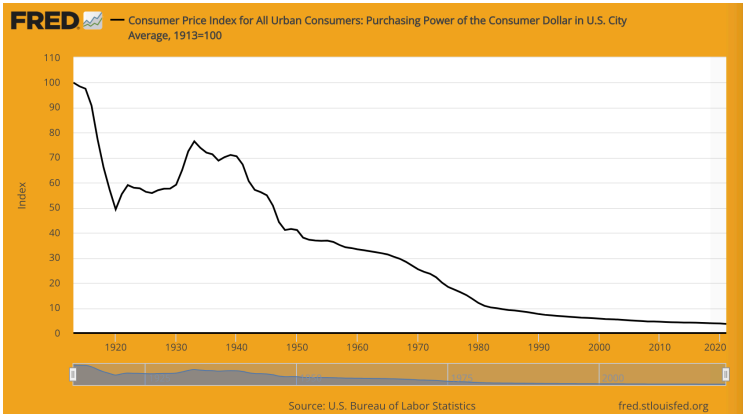


Gráfico que muestra la disminución del poder adquisitivo del dólar desde la formación de la Reserva Federal en 1913. La tasa de inflación acumulada desde 1913 ronda el 2.525,4%. Todas las monedas fiat de los bancos centrales de todo el mundo están siguiendo un ritmo de caída similar.

- **Cuanto más dinero se crea de la nada, más pierde su valor.**
- A esto se le llama **inflación.**
- La inflación es un **robo de tiempo,** literalmente. El valor de tu tiempo te es arrebatado cuando lo guardas en una moneda que está inflada y manipulada.
- La inflación es también un **impuesto oculto**
- Este robo de tiempo y los impuestos también afectan al dinero fiat de todos los demás países, ya que están vinculados al dólar estadounidense, que ha sido la moneda de reserva mundial desde el acuerdo de Bretton Woods de 1944.

- **En EE.UU., una tasa de inflación anual del 2% está incluida en el mandato de la Reserva Federal.**
- Esto significa que está **GARANTIZADO que podrás comprar un 2% menos** con el mismo billete de 20 dólares cada año.
- **En febrero de 2022, la tasa de inflación anual fue del 7,9%** (mucho más del 2%), lo que significa que perdiste el 7,9% de su poder adquisitivo en el último año.
- Dicho de otra forma, esto significa que, de media, las cosas subieron de precio un 7,9%.
- Así que, si llenar la cesta de la compra te costó 50 dólares en 2021, la misma cesta te costaría 53,95 dólares en 2022.
- **Si se midiera la inflación de forma precisa, como se hizo a principios de la década de 1980, en realidad estaría más cerca del 15% ahora, en 2022, y el valor de tu cesta de la compra sería de 57,50.**
- **Cuando se observa por categorías, se puede ver que la inflación es en realidad mucho peor que del 7,9% en muchas categorías durante el último año:**

- Energía - 25,6%
- Gasolina - 38%
- Vehículos nuevos - 12,4%
- Coches y camiones usados - 41,2%
- Alimentos - 7,9% (la más alta desde Julio de 1981)

Promedio de Inflación en los
últimos 50 años en los EE.UU.:

Coste Medio	1971	2021	% de incremento
Salario	$9,400	$53,400	469%
Casa	$23,400	$408,000	1,643%
Galón de Gasolina	$0.36	$3.60	1,000%
Coche Nuevo	$3,400	$39,000	1,047%
Título Universitario	$1,400	$26,000	1,757%
Cesta de la Compra	$20	$133	565%
Electricidad/kWh	$0.02	$0.14	600%

Historia Real:
~ Se adquirió una casa en 1976 por 58.000 dólares.
~ Al contabilizar la inflación "oficial" esto serían 279.000 dólares en 2022.
~ En 2022, la misma casa fue valorada recientemente en 2,09 millones de dólares.
~ Piense sobre esto…

- **A medida que aumenta la inflación, tus ahorros (si es que tienes la suerte de tenerlos) pierden valor.**

- Con el tiempo, pierden MUCHO valor.

- Si hoy comenzaras a ahorrar 100 dólares cada mes, con la mejor tasa de interés disponible del 0,05%:
  - Dentro de 30 años, habrías ahorrado 84.019 dólares.

- Ajustado a la inflación del 2% exigida por la Reserva Federal:
  - Dentro de 30 años, tus **ahorros tendrían un poder adquisitivo efectivo de tan sólo 46,384 dólares.**

- Si lo ajustamos a la inflación "actual" del 7%:
  - ¡Tus ahorros por valor de 84.019 dólares tendrían un poder adquisitivo de sólo 11.037 dólares en 30 años!

- **En efecto, esto significa que te han robado unas seis o siete horas de trabajo = Robo de tiempo.**

Otra forma de verlo es la siguiente:

- En 1971, el coste de una casa = 2,5 veces un salario anual promedio.
- En 2021, el coste de una casa = 8 veces el promedio de un salario anual promedio.
- En 1971, un coche nuevo costaba sobre 1/3 de un salario medio.
- En 2021, un coche nuevo costaba cerca de 2/3 de un salario medio.

Confío en que ahora quede
claro que la inflación
no juega
a tu favor.

Nota: Estos números son promedios, y pueden variar dependiendo de muchos factores. La idea es la misma: la inflación se ha disparado y no muestra signos de desaceleración, gracias a la continua impresión de dinero. La inflación es un impuesto oculto y es un robo de tiempo de nuestro trabajo y producción reales

El dinero duro arregla esto.

Bitcoin es dinero duro.

NECESITAMOS bitcoin

PARA SUSTITUIR A UNA ECONOMÍA CENTRALIZADA, MANIPULADA Y BASADA EN LA DEUDA

No creo que volvamos a tener una buena economía, a no ser que antes se la quitemos de las manos al gobierno, pero no podemos arrebatársela por la fuerza, lo único que podemos hacer es introducir, de manera astuta, algo que ellos no puedan parar.

~ Friedrich Hayek
~ economista austríaco, filósofo y autor

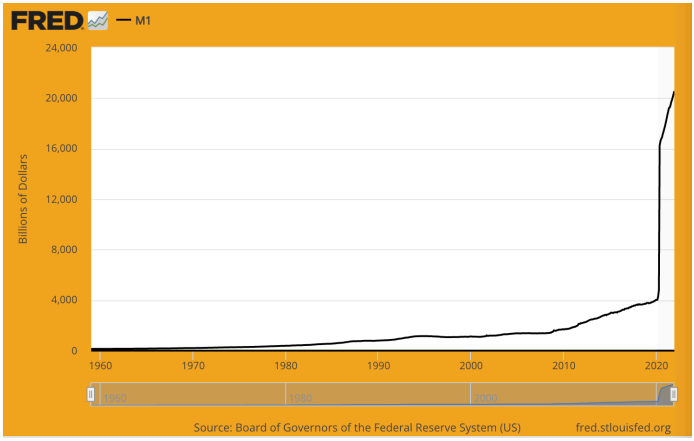


Gráfico que muestra el aumento del suministro de dinero M1, ¡de 4 trillones a más de 20 trillones de dólares desde marzo de 2020!

Echa un vistazo a esto, te hará estallar la cabeza: https://usdebtclock.org/

- **El 45% del dólar estadounidense ahora existente fue impreso en los últimos 21 meses, ¡desde abril de 2020 a enero de 2022!**
- Pero fue creado de la nada, ¿recuerdas?
- El dinero fiat está controlado por el estado, y la oferta es fácilmente manipulable.
- **La deuda nacional de EE.UU tardó 205 años en alcanzar el billón de dólares** (1776-1981)
- ¡Y tardó tan sólo **31 años** más en alcanzar los **30 billones de dólares!** (1981-2022)

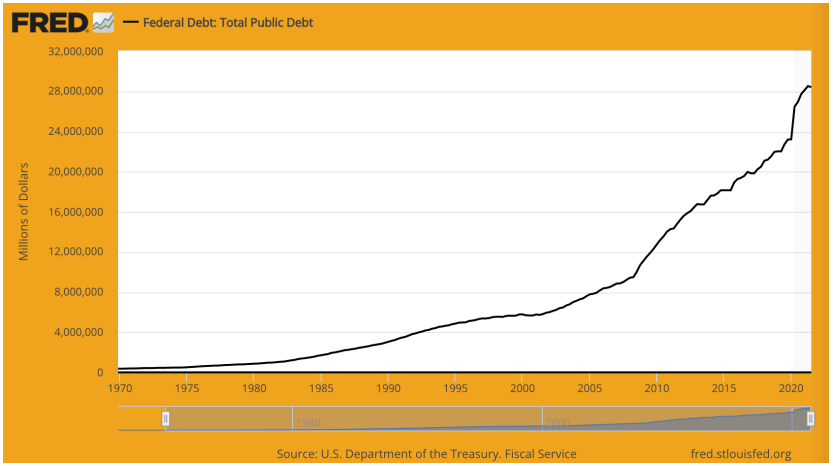


Gráfico que muestra la deuda pública total en EE.UU, desde 1970 hasta 2021.

> *La deuda mundial, medida por el Instituto de Finanzas Internacionales, asciende ahora a 303 TRILLONES de dólares. Este es nuestro mundo, con dinero fiat basado en la deuda. Por cierto, el PIB mundial es tan sólo de 84 billones de dólares.*
>
> *~ Nik Bhatia, Autor de 'Layered Money', 2021*

Como referencia:

Si tienes:	Puedes gastar 1 dólar/segundo:	
US $1 millón	durante 11 días	= 11 días
US $1 billón	durante 11.680 días	= 32 años
US $1 trillón	durante 11,680.000 días	= 32.000 años

Todos estamos a merced de quienes tienen el poder de decidir cuándo imprimir más dinero, y qué tasas de interés cobrar.

Si la Reserva Federal aumenta las tasas de interés, obtener un préstamo para comprar una casa o un coche se vuelve repentinamente más caro, lo cual ralentiza el gasto y conduce a la estanflación (estancamiento con inflación).

Si las tasas se mantienen bajas de manera artificial, se entra en un período de depresión

Permitir que el Banco Central cree un "clima" financiero, nos quita la libertad de dejar que el mercado decida qué tiene valor y qué no lo tiene.

Además de esto, cuando rescatan bancos y corporaciones, impulsan la economía de manera artificial. Es sólo cuestión de tiempo antes de que caiga el castillo de naipes.

El principal argumento para tener un banco central era que se tenía que tener a un prestamista de último recurso para cuando se tambalease la economía.

Como resultado, esto ha convertido al Banco Central en un regulador de primera instancia, **con un poder sin parangón, no votado por nadie y, en última instancia, autoritario.**

Todo el dinero es político, excepto Bitcoin. Las divisas fiat, instrumentos bancarios, créditos fintech, otras criptodivisas e inclusive el oro están controlados por los gobiernos, corporaciones, o grupos pequeños. Tener una excepción será muy útil de cara al futuro.

~ Alex Gladstein @gladstein
Director de Estrategia de la Fundación de los Derechos Humanos.

Bitcoin une a 8 millones de personas, a cien millones de empresas, sincroniza el mundo a través de jurisdicciones políticas, devuelve la racionalidad al sistema financiero, y los derechos de propiedad a la raza humana.

~Michael Saylor, CEO Microstrategy

NECESITAMOS bitcoin PARA PROPORCIONAR UN BANCO A AQUELLOS QUE NO LO TIENEN

Para 953 millones de personas con monedas debilitadas, Bitcoin representa algo más que un activo de tesorería. Para ellos, es más bien un arca de energía cifrada para escapar del diluvio.

~ Michael Saylor
CEO of Microstrategy

- Aproximadamente el 30% de la población adulta en el mundo no tiene banco, ¡eso son unos 1.900 millones de personas!

- Esto significa que no cuentan con acceso a servicios bancarios, no pueden hacer uso de los cajeros automáticos, tarjetas de débito, crédito, o cheques.

- Además de esto, no pueden obtener préstamos para iniciar un negocio, comprar un coche, una casa, etc.

- Enviar o recibir dinero, o cobrar cheques resulta caro.

- Tienen que recurrir a servicios de transferencia de dinero o cobro de cheques como Western Union, que cobran tarifas elevadas, y tardan en procesarse.

- Resulta especialmente **caro para las personas que envían dinero a sus familias que residen en otros países** (remesas), y que pueden costar hasta un 10%.

- Esto resulta también caro para las personas que reciben estas remesas, además de requerir mucho tiempo. Para recibir el dinero enviado por sus familiares, tienen que pagar el transporte e ir a la oficina de transferencia de dinero que, a menudo, está lejos de sus hogares.

- Y, en ocasiones, no es seguro para ellos desplazarse hasta estas oficinas.

- ¡Bitcoin proporciona la solución inmediata a estos problemas por medio de la Red Lightning!

#bitcoin soluciona esto

¿En qué momento se ha detenido a una tecnología
que otorga poder a las personas?

~Jeff Booth
autor de: "El Precio del Mañana"

NECESITAMOS bitcoin

PARA AYUDAR A LA GENTE A ESCAPAR DE LA TIRANÍA Y EL COLAPSO DE LA DIVISA

- Como hemos visto estos últimos meses, los gobiernos pueden, y de hecho, congelan las cuentas bancarias de aquellos con los que no están de acuerdo.

- **Esto demuestra que, en esencia, tu dinero del banco no es más que un pagaré que te pueden robar en cualquier momento.**

- Además, cuando se dispara la inflación, como estamos viendo en el caso de Venezuela, Sudán, Líbano, Siria, Argentina, Zimbabue, Turquía y otros países, los ahorros de la gente se esfuman de la noche a la mañana, y no hay nada que puedan hacer al respecto.

- Para cualquier persona que está experimentando cualquiera de estas situaciones, **Bitcoin se convierte en una solución real e inmediata a un problema que, de otro modo, sería irresoluble.**

- **Teniendo en cuenta que tanto la tiranía como la inflación van en aumento en muchos lugares, una forma prudente de protegerse de ellas, sería comprando bitcoin ahora.**

NECESITAMOS bitcoin PARA EVITAR LAS CBDC

- Es posible que hayas escuchado que los bancos centrales están empezando a crear Monedas Digitales de Banco Central (las siglas en inglés corresponden a CBDC, Central Bank Digital Currency). En mayo de 2020, 35 países **estaban explorando** esta opción.

- En el momento de escribir este libro, febrero de 2022, un total de 87 países estaban estudiando activamente o ya habían puesto en marcha un CBDC.

- En EE.UU esto se conoce como Proyecto Hamilton.

- **Las CBDC se asemejan bastante al dinero electrónico que ves en tu cuenta bancaria online, salvo que al ser "nativos" digitales, son programables, y 100% controlables.**

Una diferencia clave de los CBDC, es que los bancos digitales tendrían **control absoluto…**

~ Agustín Carstens, Director General del BPI (Banco de Pagos Internacionales)

- **Esto significa que el gobierno puede programar una fecha de caducidad para tu dinero,** obligándote a gastarlo antes de que éste caduque.

- **También pueden programarle otras cosas,** como permitir que sólo se pueda gastar en determinadas tiendas, páginas web o jurisdicciones.

- Podrían vincularla a: **tu gasto de crédito,** tu tarjeta sanitaria, **tu DNI (Documento Nacional de Identidad),** etc.

- Sumado a esto, pueden programar las restricciones que consideren oportunas **en función de tu gasto en un área determinada, o tu "gasto total", o** de lo que consideren que necesita la economía.

- Además, podrán estar al tanto de cualquier movimiento que hagas con tu dinero.

Hoy en día, no sabemos quien se gasta un billete de 100 dólares o de 1000 pesos. La diferencia clave con el CBDC es que **el banco central tendrá un control absoluto sobre las normas y reglamentos que determinan el uso de esa expresión de la responsabilidad del banco central,** *y también tendremos la tecnología para hacerla cumplir.*

~ Agustín Carstens, Director
General del BPI (Banco de Pagos Internacionales)

Nota: Decir "esa expresión de la responsabilidad del banco central" implica que tu valor, tu fuerza vital, almacenados en forma de dinero, son en realidad "propiedad" del banco central (¡no!)

NECESITAMOS bitcoin

PARA SALVAR EL JARDÍN

Bitcoin arranca, de raíz, el MAYOR problema al que nos enfrentamos, la mentira del dinero FIAT.

Esta es la mentira del dinero fiat corrupto, la usura y todo lo que conlleva para robar tu tiempo, mientras enriquece a aquellos más cercanos a la impresora del dinero (esto se conoce como efecto Cantillon)

La mentira del dinero fiat es como una mala hierba gigante en tu jardín: absorbe todos los nutrientes del suelo, **mata a las raíces** y bloquea la luz del sol, de modo que otras plantas tienen dificultad para crecer y sobrevivir.

De repente, cuando esta monstruosa mala hierba desaparece, ¡aparece la Verdad!

Todas las **plantas (personas)** comienzan a recuperarse.

El suelo **(que sería la creatividad de la gente, los bienes y servicios)** puede regenerarse.

Las raíces **(la auténtica conexión entre las personas)** volverán a crecer.

¡Y la luz del sol **(la fuerza vital)** volverá a brillar sobre nosotros!

NECESITAMOS bitcoin PARA REPARAR EL MUNDO

- Esto no es una broma. **#bitcoinfixesthis** es un meme que circula en BT (Bitcoin Twitter) por una buena razón.

- Esto puede sonar algo **"soberbio",** así que permíteme explicarlo. Cuando uno se para a pensar en "cómo están las cosas", incluso antes de 2020, cualquiera podría ver que hay "algo que no está bien".

- Destrucción desenfrenada, degradación del medio ambiente, familias y comunidades divididas, pérdida de culturas, lenguas y tradiciones, aumento de la pobreza, concentración de la riqueza en manos de unos (muy) pocos, consumismo excesivo, dinero infinito que **respalda a los políticos,** falta de alimentos y agua potable para millones de personas, obesidad y trastornos autoinmunes cada vez más frecuentes, guerras aparentemente interminables…

- Uno podría pensar que con el crecimiento exponencial de las ONGs, las organizaciones sin ánimo de lucro, las fundaciones benéficas y las llamadas instituciones respaldadas por el gobierno, estos problemas serían cada vez menos graves.

- Por el contrario, **se están agravando cada vez más.**

bitcoin SOLUCIONA ESTO

INCLUSIÓN FINANCIERA

- **Con bitcoin, todo el mundo tiene acceso al mismo sistema financiero, con las mismas reglas para todos.**

- Sin lagunas, sin irregularidades, sin tratos especiales para nadie.

- Todos tienen la posibilidad de ser compensados por el valor que aportan con el mismo dinero real, creado y mantenido con las mismas reglas.

- **Bitcoin es accesible para cualquier persona, sin importar dónde esté, con una conexión a internet.**

AÑADIENDO VALOR AL MUNDO*

- Bitcoin incentiva a la gente a aportar valor real a la comunidad y al mercado, ya que es la única manera de ganar más dinero.

- **Si uno se conforma con menos, sigue beneficiándose de trabajar por un salario justo. Y cuando uno ahorra, esos ahorros mantienen su valor a lo largo del tiempo.***

bitcoin SOLUCIONA ESTO

EL MEDIO AMBIENTE

- El dinero sólido, con una oferta limitada, crea una dinámica muy diferente a la que vemos hoy en día.*
- En lugar de un impulso irrefrenable de consumismo sin control para pagar intereses y préstamos que al final nunca se pagan, Bitcoin propone una vía de escape hacia un mundo de baja preferencia temporal.
- La destrucción desenfrenada del medio ambiente se sustituye por menos consumo, menos residuos y un enfoque considerado de la producción, en el que el mercado decide lo que tiene verdadero valor y, por tanto, las cosas se construyen para que duren
- ¡Esto es un beneficio neto para las personas, las plantas y los animales!

bitcoin SOLUCIONA ESTA GUERRA

- El sistema de dinero fiat es lo que hace que las "guerras eternas" sean posibles y rentables. Dado que la mayoría de la gente no sabe cómo funcionan los gastos de guerra, ni de dónde procede el dinero para éstas, hay poca o ninguna responsabilidad por parte del gobierno. Las guerras pueden prolongarse durante años en lugares remotos, sin ninguna supervisión real.

- Desde Vietnam, las guerras se han convertido en "guerras de tarjeta de crédito" **(me quito el sombrero, @AlexGladstein),** ya que el gobierno pide prestado dinero para financiar las guerras, y luego pide más para pagar los intereses de los préstamos iniciales.

- **En un patrón bitcoin, se requeriría que la gente de un país estuviera dispuesta a ayudar a pagar una guerra. Probablemente sólo lo harían si fuera absolutamente necesario, para defender a su familia y su país, con un objetivo final en mente.**

- Dado que no habría beneficios indebidos, los funcionarios del gobierno y las empresas no estarían incentivados para promover o participar en la guerra como una opción viable.

- **En lugar de ello, aumentarían los esfuerzos para encontrar maneras de llegar a soluciones pacíficas y de bajo coste.**

bitcoin SOLUCIONA ESTO

PREFERENCIA TEMPORAL

- La alta preferencia temporal conduce a la destrucción personal, social y medioambiental. Cuando nuestro dinero pierde valor cada día, nos vemos "obligados" a gastarlo lo antes posible, antes de que pierda más valor. Cuando nuestro tiempo está devaluado por una divisa fiat en constante inflación, perdemos la conexión con el valor de nuestro tiempo.

- Esto conduce a la desconexión y a un aumento del estrés.

- Los intentos de aliviar el estrés y encontrar un sentido se distorsionan y se convierten en distracciones, como el consumo excesivo de drogas, alcohol, compras, pornografía, comida rápida, poca capacidad de atención, adicción a las pantallas/redes sociales, etc.

- **Por otro lado el dinero, que mantiene su valor a lo largo del tiempo y mide adecuadamente nuestras contribuciones a través de nuestro trabajo, conduce a una baja preferencia temporal, una calidad de vida reflexiva, menos consumo, una conexión y conversación más profunda, y una mayor creatividad.**

¿QUÉ ES bitcoin?

Escribir una descripción de esta cosa (Bitcoin) para el público en general es muy difícil. No hay nada con lo que relacionarlo.

~ Satoshi Nakamoto, 5-7-2010

La circulación total será de 21,000.000 de monedas. Serán distribuidas a los nodos de la red cuando creen bloques, con la cantidad dividida a la mitad cada 4 años:

Primeros 4 años: 10,500.000 monedas

Siguientes 4 años: 5,250.000 monedas

Próximos 4 años: 2,625.000 monedas

Siguientes 4 años: 1,312.000 monedas Etc

Cuando se agote, el sistema puede soportar comisiones de transacción si es necesario. Se basa en la competencia de mercado abierta, y probablemente siempre habrá nodos dispuestos a procesar las transacciones de manera gratuita.

~ Satoshi Nakamoto, 9-1-2009

- Bitcoin es el dinero de la libertad…en el sentido de que tiene la capacidad de liberarnos a todos de la manipulación y el control del sistema de banca central.
- En bitcoin, las reglas monetarias son las mismas para TODOS, en TODAS PARTES.
- Bitcoin es inclusivo, en el sentido de que cualquier persona con una conexión a internet puede participar en la red y tiene que jugar con las mismas reglas.

bitcoin Es:

- DESCENTRALIZADO
- VERDADERAMENTE ESCASO
- RESISTENTE A LA CENSURA
- UN LIBRO DE CONTABILIDAD DISTRIBUIDO
- INCORRUPTIBLE

¡Estas primeras cinco propiedades distinguen a bitcoin de cualquier otra criptomoneda!!

- NO NECESITA PERMISOS
- AUDITABLE
- TRANSPARENTE
- INMUTABLE
- SIN FRONTERAS
- DIFÍCIL DE FALSIFICAR
- SEUDÓNIMO
- SIN FRICCIONES
- NO NECESITA CONFIANZA
- DE IGUAL A IGUA: [PEER-TO-PEER]

- **Bitcoin está descentralizado.**
- **Se ejecuta en miles de nodos en todo el mundo, por miles de personas que no se conocen entre sí.**
- Ninguna persona, gobierno o empresa puede controlarlo.
- Tú también puedes ejecutar un nodo, es fácil ;)
- Al tener tu propio nodo, ayudas a proteger la red y, al mismo tiempo, puedes verificar tus propias transacciones.

No confíes. Verifica.

Bitcoin (con "B" mayúscula) es una red monetaria

bitcoin (con "b" minúscula) es la divisa, o activo monetario, que se emite y ejecuta en la red Bitcoin.

Bitcoin es un gran incentivador.

La genialidad de Satoshi fue tal que por primera vez, en Bitcoin, se incentiva tanto a los buenos como a los malos actores a seguir las reglas.

Los incentivos pueden ayudar a los nodos a actuar de forma honesta. Si un atacante codicioso logra reunir más potencia de CPU que todos los nodos honestos, tendría que elegir entre usarla para robar a la gente, o usarla para generar nuevas monedas. Debería encontrar más rentable seguir las reglas, esas reglas que lo favorecen con más monedas nuevas que a todos los demás juntos, que socavar el sistema y la validez de su propia riqueza.

~ Satoshi Nakamoto, 31-10-2008

- **Bitcoin es el primer dinero nativo digital.**
- A diferencia de tu cuenta corriente online, **que es solamente una forma digital del dinero fiat del banco central…**
- Bitcoin es una divisa digital descentralizada.
- Bitcoin no tiene una **autoridad central.**
- Bitcoin no pertenece a **ningún estado.**
- Considera las implicaciones…

Bitcoin es una divisa digital descentralizada que permite pagos instantáneos a cualquier persona, en cualquier parte del mundo. Bitcoin utiliza la tecnología peer-to-peer [de igual a igual para operar sin una autoridad central: la red realiza la gestión de transacciones y la emisión de dinero se lleva a cabo de forma colectiva.

~ Bitcoin Wiki
en.bitcoin.it

 Bitcoin es el dinero mágico de internet.

 No, en serio, **Bitcoin es la forma en que vamos a arreglar el mundo.**

 ¿En serio? Sí.

Bitcoin es una forma de transferir valor:

- De cualquier cantidad
- De forma segura
- Al instante (en la red Lightning)
- Entre dos partes
- En cualquier momento
- 24/7
- En cualquier lugar
- Sí, en cualquier lugar
- Piensa en eso.

Con una divisa electrónica basada en pruebas criptográficas, sin la necesidad de confiar en un intermediario externo, el dinero puede estar seguro y las transacciones no requerir esfuerzo.

~ Satoshi Nakamoto, 11-2-2009

Con certeza, mover Bitcoin es (casi) gratuito. Estoy seguro al 100% de lo que estoy recibiendo.

~ Michael Saylor, Director General de Microstrategy

- Puedes enviar 1,13 dólares, 46c, 359 sats, 500,000.000 de sats, o 1 millón de dólares a cualquier persona, en cualquier lugar, en cualquier momento...de forma instantánea y casi gratuita, a través de la red Lightning, construida sobre Bitcoin.

- **Y nadie te puede detener.**

- ¿Puedes hacer eso con el oro, plata, USD/GBP/EUR/YEN/CYK/ZAR o cualquier otra moneda fiat del banco central? (No)

Bitcoin es histórico. Esta es la primera vez en la historia que se crea un sistema monetario verdaderamente descentralizado, resistente a la censura, inmutable, sin fronteras, permisos, e incorruptible y con un tope (21 millones de monedas).

Bitcoin es tan importante para descentralizar el poder y aumentar la inclusión financiera, como lo fue la invención de la imprenta, y más tarde, la de la **World Wide Web, para descentralizar y aumentar el acceso a la información.**

Mucha gente descarta automáticamente la moneda electrónica como una causa perdida debido a todas las empresas que fracasaron desde los años 90. Espero que sea obvio que lo único que las condenó fue la naturaleza de control centralizado de esos sistemas. Creo que es la primera vez que estamos probando un sistema descentralizado y no basado en la confianza.

~ Satoshi Nakamoto, 15-2-2009

- **Bitcoin es un libro de contabilidad distribuido, descentralizado, transparente e inmutable.**

- Lo que simplemente significa que es una forma en la que cualquier persona puede ver quién posee qué en un momento dado, y no se puede cambiar.

- Excepto que el "quién" no es un nombre, sino una dirección compuesta por números y letras.

- Un ejemplo de una dirección de bitcoin:

  bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq

- **Bitcoin es, por tanto, seudónimo.**

Bitcoin es:

- Un emisor imparcial de activos
- Una reserva de valor
- Un medio de intercambio
- Y próximamente, una unidad de cuenta
- **Así como**
- **El fin del intercambio**

Es el emisor, el oro, el efectivo, la tarjeta de débito Y paypal, el banco, Venmo, CashApp, Western Union.

¡TODO EN UNO!

Bitcoin es un sistema de registro que usa matemáticas e informática en lugar de banqueros, contables y contadores.

Elimina a los intermediarios, los bancos, gobiernos, **comisiones por sobregiro/descubierto, comisiones de las cuentas corrientes,** horas limitadas de servicio, posibilidad de censura, cuentas congeladas, manipulación de la oferta monetaria, tasas de interés, el Fondo Monetario Internacional (FMI), el Foro Económico Mundial (FEM), las tiendas físicas, edificios, cajeros automáticos, cheques, corrupción, usura, petrodólar, eurodólar, señoreaje, bonos, acciones, banca de reserva fraccionaria, Visa, Mastercard, American Express, Western Union, Banco de Pagos Internacionales (BIS), los días de espera para que se realice una transferencia bancaria.

En lugar de tener a alguien entre tú y la persona con la que quieres acordar algo, puedes hacerlo directamente, sin nada de por medio.

¡No necesitas pedir permiso para enviar tu propio dinero!

¡Ahora puedes hacerlo como, cuando y dónde tú elijas, con liquidación inmediata!

En pocas palabras…

- **Bitcoin es una propiedad digital que nadie te puede quitar.**

- Tener bitcoin significa tener derecho a enviar valor desde una dirección específica que controlas con tu clave privada, a CUALQUIER otra dirección que elijas.

- *Bitcoin es un derecho de propiedad que es independiente del monopolio de la violencia.*

~ Robert Breedlove, @breedlove22

- ¡Además, podemos reutilizar decenas de miles de edificios bancarios en todo el mundo para convertirlos en centros comunitarios, bibliotecas, salas de conciertos, de exposiciones/galerías de arte, y cualquier otra cosa que podamos imaginar para enriquecer y animar la comunidad!

- Bitcoin es un evento único en su especie.

- El descubrimiento de Bitcoin hace 14 años, es para la libertad y la soberanía financiera humana, como lo fue el descubrimiento del fuego para el florecimiento de la humanidad hace más de 500.000 años, y la imprenta para descentralizar el acceso al conocimiento humano, hace casi 900 años.

- Bitcoin es una opción.

- Bitcoin crea soberanía.

- **Bitcoin es una verdadera reserva de valor.**

- Almacena tu recurso más preciado, tu tiempo, de forma que puedas acceder a él más adelante.

> *Bitcoin es como un conducto de energía de gran ancho de banda para tu yo del futuro…puedes trabajar hoy, y Bitcoin congelará tu energía para su uso posterior.*
>
> ~ Robert Breedlove

> *La raíz del dinero es el tiempo, y la raíz del tiempo es el valor.*
>
> ~ Guy Swann

- Bitcoin es una **cadena temporal,** literalmente.
- Puedes medir el tiempo en bloques, ya que un bloque se mina cada 10 minutos.

- **Nuestro tiempo es nuestro recurso más escaso y preciado.**
- **Es nuestra fuerza vital, literalmente.**
- **¡El dinero de verdad nos permite almacenar nuestro tiempo!**

- Es la manera de reconocer el tiempo que "gastamos".
- Cambiamos nuestro tiempo por dinero, **el cual no es más** que un registro de nuestro tiempo y esfuerzo.
- Esta capacidad de preservar nuestro tiempo de manera que tengamos "acceso" a él más adelante en la vida, cuando ya no seamos capaces de trabajar como antes, es magia.
- **Cuando se produce la inflación, ésta nos roba el valor de nuestro tiempo.**

- Bitcoin es una **reserva de valor.**
- Bitcoin es un **medio de intercambio.**
- Un día, bitcoin **será una unidad de cuenta.**
- Un día, bitcoin **será LA unidad de cuenta.**

- **Bitcoin es escaso.**
- Cuenta con un límite de 21,000.000 de monedas.
- Nunca volverá a haber más.
- El código aquí es ley*

* Si bien es "técnicamente" posible cambiar el código, la genialidad de Satoshi lo impide, ya que aumentar (inflar) el suministro sólo serviría para disminuir el valor de todas las monedas en circulación. Por lo tanto, esto incentiva a todos a aceptar de forma implícita mantener el suministro de 21,000.000.

Bitcoin puede dividirse de manera infinita.

Actualmente, es divisible al octavo decimal: 1,00000000

Hay 100,000.000 de satoshis en 1 bitcoin.

1 satoshi = ₿ 0.00000001

Puedes comprar sats (satoshis) en cualquier cantidad.

- **Bitcoin es el dinero más duro y sólido que hemos conocido.**
- Es incluso más sólido que el oro, ya que este no se puede dividir tan fácilmente, ni es portátil, **tiene poca velocidad de transmisión (se mueve lentamente) y no es fácil de verificar.**
- **Bitcoin tiene las propiedades monetarias más superiores que cualquier activo jamás conocido.**

Propiedades del dinero	Bitcoin	Oro	Dinero Fiat
Verificabilidad escasa	✓	✗	✗
Fácil de transportar	✓	✗	✗
Verificable al instante	✓	✗	✓
Fácilmente divisible	✓	✗	✓
Duradero	✓	✓	✗
Utilizable en todas partes	✓	✓	✗
Resistente a la censura	✓	✗	✗
Difícil de falsificar	✓	✓	✗
Alta velocidad	✓	✗	✓

Bitcoin es el antídoto.

Intentar "estabilizar" la economía con rescates, impresión de dinero, Flexibilización Cuantitativa (QE) y manipulación de la tasa de interés es como **mantenerla viva de manera artificial, con una máquina.**

Esta "máquina" sólo puede durar un tiempo, antes de que su mantenimiento se vaya volviendo cada vez más caro, y al mismo tiempo, menos sostenible, lo que llevará a un colapso.

Bitcoin soluciona esto.

Bitcoin es un dinero mejor.

- **Bitcoin es antifrágil**

- Y lo es aún más con cada intento de ataque, con cada prohibición del gobierno, con cada FUD (Fear, uncertainty and Doubt, Miedo, Incertidumbre y Duda) de los medios de comunicación dominantes.

- Bitcoin nunca ha sido hackeado*

- Aunque muchos lo han intentado.

* Aunque hayas oído hablar de hackeos, son los intercambios los que han sido hackeados.

Recuerda: Ni tus llaves, ni tus monedas.
>> Retira siempre tus sats a tu propia billetera. Y lo mejor es comprar peer-to-peer [de igual a igual] >> Bisq sirve para esto, por ejemplo. ¡Sin duda merece muchísimo la pena aprender cómo hacerlo!

- Bitcoin es una combinación de :
    - Criptografía
    - Matemáticas
    - Networking/Redes
    - Teoría de Juegos
    - Incentivos económicos…
- … que cooperan para generar confianza en un entorno descentralizado y sin confianza para apoyar a una divisa digital segura.

- **Bitcoin es una madriguera de conejo** muy, muy profunda, lo cual te hace preguntarte casi todo lo que creías saber ;)

- Bitcoin es autónomo.

- **Bitcoin es, simplemente, Bitcoin.**

- **Bitcoin es una relación simbiótica** entre: humanos <-> una solución perfecta para transferir y almacenar tiempo/valor.

- Los humanos necesitan Bitcoin, bitcoin necesita a los humanos.

- **Bitcoin es la solución al problema de los generales bizantinos**
- Se pensaba que esto era un problema irresoluble en la ciencia de la computación.
- Este problema surge en los sistemas descentralizados, en los que se pensaba que era imposible demostrar que el "mensaje enviado = mensaje recibido", ya que el **interceptor** podría ser **actuar con malas intenciones** y falsificar el mensaje.
- En otras palabras, parecía imposible formar consensos entre una red de ordenadores distribuidos e independientes.
- Al utilizar la **marca de tiempo** junto al **libro de contabilidad distribuido de forma segura (encriptado),** Satoshi resolvió este problema.
- Su solución se conoce como **el consenso de Nakamoto.**

- **Bitcoin es la solución al problema de doble gasto.**
- Esto significa que cuando envías bitcoin, el receptor puede estar seguro de que realmente eres el dueño del bitcoin que enviaste, y que una vez enviadas, no puedes volver a gastar esas monedas enviándoselas a otra persona (doble gasto).
- Es como si yo te diera una naranja, por ejemplo.
- Una vez deja de estar en mis manos y pasa a las tuyas, yo ya no tengo esa naranja para dársela a otra persona.

Los dobles gastos nunca se aceptan en el conjunto de las transacciones, por lo que cada nodo es testigo de la transacción que vio primero al trabajar para ponerla en un bloque.

~ Satoshi Nakamoto, 9-12-2010

- Bitcoin es un activo financiero, como el dinero en efectivo o el oro, directamente en manos del portador (propietario).

- Esto significa que una vez enviado (dado) va directamente al nuevo portador (propietario), sin necesidad de intermediarios (banco) para procesar la transacción.

- Bitcoin es un protocolo P2P de igual a igual [Peer-to-peer].
- Bitcoin es resistente a la censura.
- Esto significa que nadie puede impedir o retrasar que una transacción pase al nuevo portador.
- Bitcoin fluye libremente.
- No puede haber custodios.

Bitcoin es Trustless o "Sin Confianza".

> *El problema de raíz con la moneda convencional es toda la confianza que se requiere para que funcione. Se debe confiar en que el banco central no degradará la moneda, pero la historia del dinero fiat está llena de violaciones de esa confianza.*

~ Satoshi Nakamoto, sobre la importancia de la naturaleza de la desconfianza en Bitcoin.

- **Bitcoin es código.**
- **El código es discurso.**
- Sorpréndete. Echa un vistazo a: **github.com/bitcoin**
- Entra para ver el código, las solicitudes de incorporación de cambios, las revisiones, los compromisos; por parte de los increíbles desarrolladores que están trabajando, manteniendo y mejorando la creación que es bitcoin.

Bitcoin es el internet del dinero.

Cuando uno se para a considerar que todo lo demás se está volviendo o se ha vuelto digital, incluyendo:

- Música
- Libros
- Bancos
- Películas
- Educación
- Fotos
- Llamadas telefónicas
- Mapas
- Y la lista continúa…para bien o para mal…
- Entonces uno ve que esto es, lógicamente, un paso a seguir para el dinero.

(**PERO** necesitamos BITCOIN, ¡**NO** CBDC!)

EL GENIO DE SATOSHI

Bitcoin es TODO lo siguiente:

- Un **libro de contabilidad descentralizado y distribuido.**
- Un sistema de pago.
- **Y el propio valor que se transfiere.**

Fuera de bitcoin, la creación de dinero (emisión), y la contabilidad (seguimiento del dinero recibido/gastado), está centralizada, e incluye las siguientes capas separadas.

- La **emisión de dinero** por parte del Banco Central.
- El **tipo de dinero** a negociar (oro, plata, USD/EUR/YEN/ZAR, etc.)
- La **cantidad de dinero** a negociar.
- El **libro de cuentas**, ya sea en papel o digital.
- Los **equipos de confianza** que introducen los números en los libros de contabilidad.
- Los **equipos de confianza** que mantienen la seguridad de los libros de contabilidad (físicos), o los que mantienen las bases de datos informáticas.
- Los **equipos de seguridad** de confianza que trabajan para evitar la piratería de las bases de datos.

Con Bitcoin, **¡todas estas capas se vuelven una sola!**

Aunque esto pueda sonar más centralizado, la genialidad de Satoshi lo hizo de tal manera que, lo contrario es la verdad.

¡Es 100% descentralizado!

- **Bitcoin no tiene NINGUN punto central de fallo.**

- **La única manera de que todo esto se convierta en uno solo y esté descentralizado es que el libro de contabilidad distribuido sea mantenido por un grupo de personas, global y ad-hoc, que minen y/o ejecuten nodos completos de manera voluntaria.**

- Además, los incentivos de la red animan a todo el mundo a cumplir las normas.

- ¡Puedes unirte a nosotros!

Bitcoin es una revolución pacífica

Bitcoin es esperanza

¿CÓMO FUNCIONA bitcoin?

Reglas no Gobernantes

tik-tok/
/siguiente bloque

Criptografía (sustantivo) /De cripto- y -grafía.

: Técnica para asegurar la transmisión de información privada que utiliza una escritura convencional secreta, de manera que sea ilegible para cualquiera que no posea la clave de descifrado.

~ Diccionario Enciclopédico Vox 1

Hashing (verbo):/ˈhæʃɪŋ/

: Es un método de encriptación: el proceso de utilizar un algoritmo matemático contra los datos para producir un valor numérico (a hash digest) que representa esos datos.

~ crsc.nist.gov

Recuerda:
El ecosistema Bitcoin incluye: >>
bitcoin: El activo **monetario digital**
Bitcoin: La **red de pago** de mineros y nodos.

1 bitcoin = 100,000,000 satoshis (sats)
(Puedes comprar sats, una fracción de bitcoin)

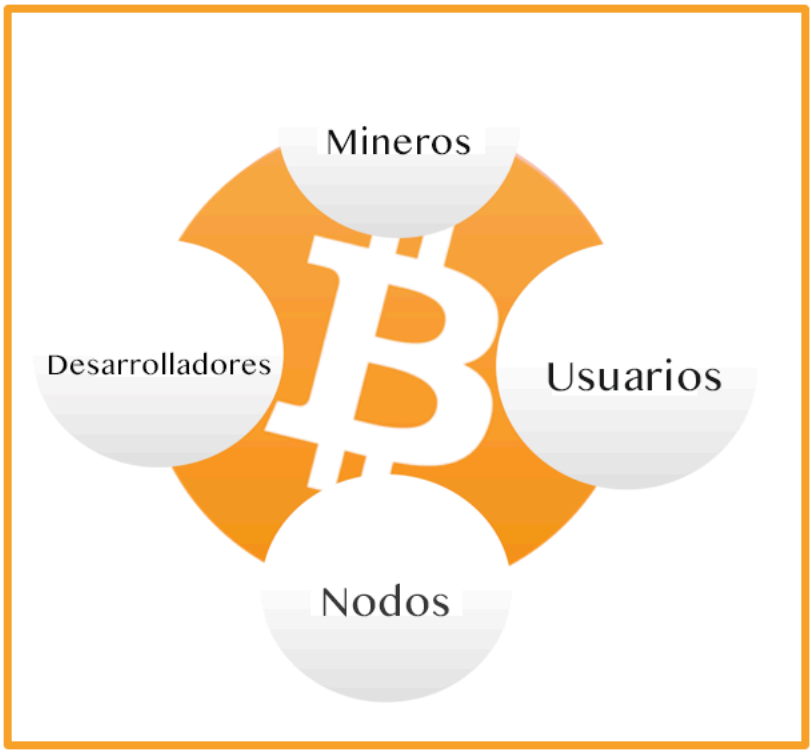
Bitcoin usa **proof-of-work, (prueba de trabajo)** criptografía de llave pública y red peer-to-peer [de igual a igual], para procesar y verificar los pagos en un libro de contabilidad global, distribuido y online.

Definimos una moneda electrónica como una cadena de firmas digitales. Cada propietario transfiere la moneda al siguiente propietario firmando digitalmente un hash de la transacción previa y la clave pública del siguiente propietario, y añadiendo ambos al final de la moneda. El beneficiario puede verificar las firmas para verificar la cadena de propiedad.

~ Satoshi Nakamoto
Bitcoin White Paper, Pt.2, 2008
Descripción de cómo funciona una transacción de bitcoin en el libro de contabilidad distribuido.

EL ECOSISTEMA DE BITCOIN..

consiste en mineros, nodos, usuarios, desarrolladores,
¡todos trabajando de forma
independiente y simultánea para dar
vida a lo que es BITCOIN!



LOS MINEROS

- Son nodos especializados (ordenadores) que "minan" los bloques que pasan a formar parte de la cadena de bloques de bitcoin (el término empleado es **bitcoin blockchain**)

- Al hacerlo, confirman las transacciones verificadas que han realizado los usuarios, emiten nuevos bitcoins y protegen toda la red.

LOS USUARIOS

- **Tú y yo**. Todos nosotros. La gente. Reconocer y apreciar el valor proporcionado, mediante la transacción, entrega y recepción **de este dinero, que nos da energía.**

- **Y podemos almacenar esta energía para más adelante, cuando sea necesaria.**

LOS NODOS

- Los nodos conforman una red descentralizada, global y voluntaria de miles de ordenadores, grandes y pequeños, cada uno de los cuales ejecuta de forma independiente la blockchain de bitcoin, verificando las transacciones (evitando así el doble gasto) y ayudando a asegurar el sistema.

LOS DESARROLLADORES (DEVS)

- Codificadores, programadores, autores digitales y videntes que trabajan para mantener la red, mejorar la seguridad, la privacidad y la interfaz de usuario, traduciendo el código a un lenguaje e imágenes que el resto de nosotros podamos comprender y usar.

EJEMPLO DE UNA TRANSACCIÓN EN BITCOIN:

Ali quiere mandarle unos bitcoin a Benji:

1. Ali **abre su app de billetera de bitcoin** en el móvil y le da a **"Enviar".**

2. Benji **abre su app** y le da a **"Recibir".**

3. **Si ambos están en el mismo lugar:** Ali escanea el código QR de la app del teléfono de Benji.

4. **Si ambos no están en el mismo lugar:** Ali copia y pega la dirección que Benji le haya enviado en el campo correspondiente de su billetera.

5. Ali **introduce la cantidad a enviar,** y le da a **"Enviar".**

6. **Unos segundos después**, Benji verá la cantidad pendiente en su billetera.

7. Si dicha cantidad fue enviada a través de Lightning, será confirmada casi al instante, y es prácticamente gratis.

8. Si la cantidad fue enviada "on-chain" (en la cadena principal de Bitcoin), incluye una pequeña tasa, y suele tardar unos 10 minutos en confirmarse. Puede tardar más tiempo, dependiendo del tráfico en ese momento.

LA CARA OCULTA DE UNA TRANSACCIÓN EN BITCOIN:

(Las definiciones de los términos se encuentran a continuación)

1. Cuando Ali envía esos sats a Benji, la **transacción se transmite** a la red.

2. **La transacción es verificada por los nodos,** que se aseguran de que Ali dispone realmente del bitcoin para enviarlo, y que no lo ha gastado antes (para prevenir el doble gasto).

3. Una vez verificado por un nodo, **espera en el mempool** junto a las transacciones de otras personas.

4. Las transacciones en el *mempool* **se añaden a un bloque** a la *blockchain* cuando un minero encuentra un nonce que satisface el **algoritmo de dificultad.**

5. **Cada bloque** tiene asignada una marca de tiempo.

6. Esto crea **inmutabilidad,** y ayuda a proteger the difficulty algorithm adjustment from being manipulated.

7. **Cada bloque representa una confirmación** para las transacciones incluidas en él.

8. Conforme se crean y añaden bloques (aproximadamente, cada 10 minutos), aumenta la inmutabilidad de la blockchain.

TRANSACCION ~ La cara oculta de una transacción en Bitcoin:

- Una transferencia de valor en forma de satoshis, de un poseedor de bitcoin a otro.

NODO ~ Una "sucursal" del "banco" de bitcoin. Cualquiera puede llevar un nodo.

- Los nodos, junto con los mineros, los usuarios y los desarrolladores, forman parte de la red peer-to-peer de Bitcoin.
- Imagina **cada nodo completo como un libro de contabilidad que contiene los saldos de cada clave privada.**
- Interactúan y llegan a un consenso (se ponen de acuerdo) entre ellos, aceptando y validando las transacciones de otros nodos, junto con los bloques de los mineros, y luego los transmiten a otros nodos.
- Los nodos son gestionados por un grupo *ad-hoc* formado por miles de voluntarios de todo el mundo. Un nodo completo es aquel que ha validado de forma independiente toda la *blockchain* de Bitcoin, desde el bloque Génesis minado por Satoshi en 2009. Actualmente se necesitan unos 2 ó 3 días y 390GB de espacio.
- Cuantos más nodos activos haya, más distribuida y por tanto, más resistente será la red en su conjunto.
- Actualmente hay más de **15.000 nodos completos accesibles** en todo el mundo, **y muchos más inalcanzables.**
- Todos los nodos participantes son iguales.

TRANSMISION ~ Hacer saber a la red que estás enviando bitcoin a alguien.

➢ Cuando haces click en "Enviar", tu billetera firma la acción de la transferencia con tu clave privada, y hace saber a todos los demás nodos tu intención de transferir valor, para que puedan guardarla.

MEMPOOL ~ Una sala de espera de transacciones

➢ Se trata de la "sala de espera" a la que se envían las transacciones validadas, para que las recoja un minero y las añada a un bloque.

BLOQUE ~ Una "página" en el libro de contabilidad de bitcoin

➢ El libro de contabilidad distribuido de Bitcoin se compone de "bloques" digitales. Cada bloque contiene transacciones de bitcoin verificadas que mantienen el libro de contabilidad global **en estado** preciso y actualizado. También contienen el **nonce** (acrónimo de "number used only once/número usado sólo una vez"), que es un **límite** de tiempo, así como un **hash** del bloque anterior, todo lo cual contribuye a la inmutabilidad de la *blockchain* de Bitcoin.

BLOCKCHAIN ~ Todo el libro de contabilidad de bitcoin

➢ El blockchain de bitcoin es el libro de contabilidad distribuido que contiene todos los bloques y transacciones de bitcoin realizadas desde que Satoshi minó el bloque Génesis en 2009.

MINEROS ~ Un nodo especializado que confirma las transacciones y emite nuevos bitcoins.

- Los mineros de bitcoin son ordenadores especializados. Dirigen una cantidad de potencia de cálculo (*hashrate*) **en una lotería digital para adivinar un número que satisfaga el algoritmo de dificultad actual,** y así "minar" un "bloque" (una parte del libro de contabilidad).
- Un bloque minado recibe una cantidad límite de tiempo y se añade a la *blockchain* (también conocida como *timechain*)

ALGORITMO DE DIFICULTAD ~ Un diseño especial y adaptable que ayuda a mantener predecible la emisión de nuevos bitcoins.

- Ésta fue una de las geniales soluciones de Satoshi para ayudar a proteger a la emisión de bitcoin de que se sobrepase a sí misma, a medida que se desarrollan ordenadores más avanzados.
- Cuando se conectan más mineros, el número objetivo (*nonce*) de la "lotería" se reduce y, por tanto, es más difícil de encontrar.
- Cuando hay menos mineros *online*, es más fácil.
- El algoritmo se **ajusta automáticamente cada 2016 bloques** (cada dos semanas, aproximadamente), para garantizar un ritmo de suministro predecible, en el que se mina un bloque aproximadamente cada diez minutos.

NONCE ~ Un número aleatorio de 32 bits

- Se trata de un número aleatorio de 32 bits que los mineros añaden al final de la lista de las transacciones con *hash*, para intentar satisfacer **el objetivo de dificultad para minar un bloque.**
- **Cuando un minero encuentra un nonce que lleva a generar un hash por debajo del número objetivo actual, ha minado un bloque, así consigue añadirlo a la blockchain, y reclamar el bloque de bitcoin como recompensa.**

LIMITE DE TIEMPO ~ Marca el tiempo

- Cada bloque minado tiene un asignado un límite de tiempo.
- Esto es para una mayor seguridad, inmutabilidad y para ayudar a **establecer el ajuste de dificultad.**

INMUTABILIDAD ~ No se puede cambiar

- Esto significa que el blockchain está **"grabado en piedra de forma digital".**

PRUEBA DE TRABAJO (PoW) ~ Prueba criptográfica de que se ha realizado un trabajo difícil para satisfacer un algoritmo.

- Los mineros usan el algoritmo PoW para demostrar que han empleado una gran cantidad de potencia computacional a través de la electricidad (trabajo), con el fin de lograr el consenso de manera descentralizada, y para evitar que los actores corruptos hagan spam en la red.

CLAVE PUBLICA CRIPTOGRÁFICA ~ Un proceso que crea las claves digitales para que accedas a tus bitcoins.

- Se trata de un sistema por el cual se crean dos claves mediante un algoritmo criptográfico
- **Una de las claves es pública:** como lo es el número de tu cuenta bancaria; puedes dárselo a la gente para que te envíen bitcoin a cambio de bienes, regalos o servicios.
- **La otra clave es privada:** sólo tú tienes una copia y la utilizas para desbloquear tu cuenta y hacer a tu bitcoin, igual que una contraseña que desbloquea tu cuenta bancaria online.

RED DE IGUAL A IGUAL -PEER-TO-PEER (P2P) ~ Una red descentralizada sin intermediarios

➢ Los nodos completos (pares) mantienen en colaboración una red de pares para la validación de bloques y transacciones. En este tipo de red, cada nodo puede solicitar/proporcionar datos a sus pares. No hay custodios.

LA RED LIGHTING ~ Una red construida con bitcoins, que permite enviar/recibir sats muy rápido, y de forma casi gratuita.

➢ Lightning es una solución de escalado de capa 2. Esto significa que proporciona una forma de escalar bitcoin, dándole el potencial de procesar millones de transacciones por segundo (TPS)

BILLETERA ~ Una "billetera" es una app de software que contiene las claves criptográficas para acceder a tu bitcoin.

➢ Puede estar en un smartphone, un ordenador, o un **pequeño dispositivo de hardware independiente.**

➢ Una billetera de bitcoin sería más bien un dispositivo de firma. Tu bitcoin nunca sale de la *blockchain*, el libro de contabilidad digital.

➢ Cuando quieres enviar o gastar tu bitcoin, la billetera firmará y transmitirá la transacción a la red, para que ésta pueda ser verificada y añadida a un bloque en la *blockchain*.

DESARROLLADORES ~ Programadores informáticos

➢ Los cypherpunks que mantienen la red, mejoran la seguridad, comprueban si hay errores, envían solicitudes de actualización, las revisan, y auditan el código.

CLAVE PUBLICA ~ Como el número de una cuenta bancaria para recibir bitcoin.

- Puedes dárselo a la gente para que te envíe bitcoin, al igual que darías tu número de cuenta a alguien para que te envíe dinero fiat.

CLAVE PRIVADA ~ Para asegurar, enviar y tener acceso a bitcoin, al igual que la llave de una caja de seguridad.

- Una clave privada de bitcoin es una **serie** secreta de números y letras que te permite enviar/gastar tus bitcoin.
- Solo tú tienes una copia. ****Es muy importante mantenerla a salvo, ya que si alguien obtiene una copia de ella, puede gastar tus bitcoin****

LIBRO DE CONTABILIDAD DISTRIBUIDO ~ libro de contabilidad mantenido por todos los que desean colaborar.

- En lugar de un libro de contabilidad controlado de forma central, e invisible para el público, como el que tiene un banco, Bitcoin es un libro de contabilidad transparente, abierto y descentralizado, visible para cualquiera, en cualquier momento.
- Las direcciones son cadenas de letras y números, sin nombres.
- Aunque se trata de un seudónimo, es posible rastrear las transiciones, especialmente si el bitcoin se compró **en un intercambio centralizado.**
- Hay que confiar en que los bancos llevan sus libros de contabilidad de forma honesta.
- La red Bitcoin, en cambio, es poco fiable y cualquiera puede auditarla en cualquier momento.

MÁS INFORMACIÓN SOBRE EL MINADO/MINERÍA

- El bitcoin es "minado" en todo el mundo por potentes ordenadores especialmente diseñados para ello, se conocen como mineros ASIC (Application Specific Integrated Circuit).

Un minero de Bitcoin Antminer S9 ASIC

- **Los mineros emplean potencia de cálculo, conocida como hashrate, a través de la electricidad de la red,** para añadir bloques a la *blockchain* de Bitcoin.
- Estos ordenadores funcionan las 24 horas del día, normalmente en conjuntos pequeños, pero los puede haber también de entre cientos o miles de ordenadores.
- Básicamente, están llevando a cabo una lotería. Cuando uno de ellos adivina una respuesta (el *nonce*), que genera un *hash* que satisface **el objetivo de dificultad actual, consigue añadir el siguiente bloque a la blockchain.**
- **Todo lo mencionado arriba es la prueba de trabajo Proof of Work (PoW) necesaria para el nacimiento de nuevos bitcoin.**

RECOMPENSA POR BLOQUE DE BITCOIN

Por su trabajo, obtienen lo siguiente:

- **Una recompensa en forma de nuevos bitcoin.**
- **Todas las comisiones de las transacciones verificadas incluidas en ese bloque.**

Cuando envías bitcoin a alguien, esa transacción incluye una tarifa y debe ser verificada por un minero, para después ser incluida en un bloque.

La **recompensa de las blockchain** de bitcoin se reduce a la mitad cada cuatro años.

Actualmente es de 6,25 bitcoins por cada bloque minado.

La próxima "reducción a la mitad" será en 2024, momento por el cual la recompensa por cada bloque minado bajará a 3,125 bitcoins.

Como ya se ha mencionado, **esto hace que se mantenga la estabilidad de emisión.**

En el año 2140, se minará el último bitcoin.

Después de que esto suceda, los mineros sólo recibirán los honorarios de las transacciones que verifiquen en cada bloque.

Dentro de unas décadas, cuando la recompensa sea demasiado pequeña, la tasa de transacción se convertirá en la principal compensación para los nodos (mineros).

~ Satoshi Nakamoto

- **Los mineros siempre serán necesarios para verificar las transacciones, manteniendo así la seguridad de la red.**
- Cada vez es más fácil para cualquiera minar en su propia casa.
- Aunque hay que ser consciente de que hay costes, y también de que la rentabilidad es baja para los mineros caseros, pero ésta es una gran forma de ayudar a asegurar y mantener la red descentralizada.

- Los mineros duran bastantes años. Por ejemplo, actualmente hay muchos Antminer S9 que llevan funcionando más de 6 años.
- Cuando los mineros se "jubilan" **pueden ser fácilmente desmontados y reciclados.**
- **¡Se están produciendo un montón de innovaciones fascinantes con gente que usan los mineros para cosas como calentar sus casas, saunas e incluso jacuzzis!**

SOBRE LA RED LIGHTNING

- **Los bloques de Bitcoin no pesan mucho (esto es intencionado),** alrededor de 1MB cada uno, lo que hace que la cadena principal de Bitcoin pueda realizar unas 7 transacciones por segundo (TPS).
- Visa tramita unas 4000 TPS.
- Además, la **primera confirmación de una transacción de la cadena principal suele tardar un mínimo de 10 minutos** (ya que se extrae un bloque cada 10 minutos, aproximadamente).
- Esto no resulta práctico si estás en una tienda y quieres pagar de forma rápida por tus productos.

* Detalle importante* La razón por la que los bloques son pequeños es para mantener la blockchain lo suficientemente pequeña para que cualquiera pueda ejecutar su propio nodo en casa, lo que ayuda a mantener la red descentralizada. Satoshi se dio cuenta de la importancia de esto: ↓

> *Los usuarios de Bitcoin podrían ser cada vez más tiranos a la hora de limitar el tamaño de los bloques de la cadena, para que sea fácil* ***(de usar)*** *para muchos usuarios y dispositivos pequeños.*
>
> ~ Satoshi Nakamoto, 10-12-2010

➢ **LEER:** "The Blocksize War" de Jonathan Bier

- Entra en escena la Red Lightning, (LN, Lightning Network en inglés), una solución de escalada de bitcoin de Capa 2.
- La "Capa 2" se refiere a que está construida sobre bitcoin.
- "Solución de escalada" significa que permite que la red:
  - ➢ Aumente enormemente la velocidad de procesamiento
  - ➢ Aumente enormemente el número de transacciones que se pueden procesar por segundo.
  - ➢ Los micropagos sean posibles.

- La Red Lightning puede considerarse (más o menos) como una cuenta que podrías mantener con algunos amigos en el bar.
- Entre todos se lleva la cuenta de quién debe qué (como un canal de la Red Lightning), y al final de la noche, el grupo salda la cuenta con el camarero (la "cadena principal").
- Los canales de Lightning pueden permanecer abiertos durante días, semanas o meses antes de ser "liquidados" en la cadena principal.

BENEFICIOS DE ⚡:

- **VOLUME** ~ El volumen de transacciones por segundo es, en esencia, ilimitado, ya que se pueden abrir innumerables canales al mismo tiempo, cada uno manteniendo su propia "ficha".

- **MICROPAGOS** ~ Puedes enviar hasta algo tan pequeño como 1 satoshi (actualmente 0,0003 dólares)

- **VELOCIDAD** ~ Normalmente se tarda entre un milisegundo y unos segundos en recibir un pago.

- **PRIVACIDAD** ~ Las transacciones no se almacenan en la *blockchain* abierta y pública de bitcoin. En cierto modo, es incluso más privado que el dinero en efectivo, porque con *Lightning,* ni siquiera la otra parte sabe necesariamente quién eres, ya que tu pago "salta" a través de diferentes canales hasta llegar al receptor. Para ser claros, no estoy diciendo que sea 100% imposible de descubrir, sólo lo es mucho más que con los pagos de la cadena principal de bitcoin (*mainchain* en inglés). Llevaría una inmensa cantidad de tiempo y energía para llegar a establecer con certeza quién le estaba haciendo pagos a quién, y no siempre sería posible hacerlo.

  ➢ **Disfruta de una forma asombrosa de visualizar la Red Lightning** en: lnrouter.app/graph

Bitcoin no puede escalar por sí mismo para que todas las transacciones financieras del mundo sean transmitidas a todas partes e incluidas en la blockhain. Es necesario que haya un nivel secundario de sistemas de pago que sea más ligero y eficiente.

~ Hal Finney, 30-12-2010
Uno de los primeros *cypherpunks* y la segunda persona en ejecutar Bitcoin

Piénsalo de esta forma:

- Bitcoin: **Cuenta de ahorros** ~ Transacciones más lentas para cantidades más grandes
- Lightning: **Cuenta corriente** ~ Transacciones muy rápidas para cantidades menores.

Bitcoin mejorado por Lightning puede considerarse tanto un producto (propiedad digital) como un servicio (red monetaria abierta). La capacidad de transferir energía monetaria a través del tiempo y el espacio sin la intervención del gobierno o la banca convencional es enormemente valiosa para la humanidad.

~ Michael Saylor @saylor
CEO Microstrategy

COMO USAR bitcoin

Bitcoin: (verbo) /bɪtkɔɪn/

Propongo hacer de "Bitcoin" un verbo que haga referencia a participar en el ecosistema de Bitcoin.

Bien, ahora que, con un poco de suerte, te habrás tomado la pastilla naranja y estarás preparado para convertirte en tu propio banco, participando en el primer dinero libre global del mundo, ¡viene la parte divertida!

CONVERTIRTE EN TU PROPIO BANCO

Aquí es donde radica el **cambio realmente épico** para volverse financieramente autosuficiente, y puede llevar tiempo comprender por completo lo que ello significa.

Se requiere de **cierta intención y dedicación para entender cómo hacerlo de la manera más segura posible.**

Para que este libro siga manteniendo la esencia de ser "el libro de bitcoin más simple jamás escrito", voy a ofrecerte un resumen aquí, más luego unos recursos al final, para que te sumerjas en ellos, que van mucho más allá del alcance de este manual.

HODL: (verbO) /ho'dill/

:Conservar tu bitcoin
: No venderlo

(Es de un post de bitcointalk.org de 2013, donde la persona que lo posteó decía estar borracha y escribió mal "HODL"- Búscalo en Google, vale la pena leerlo ☺)

Si bien la red sigue creciendo, hay mucho valor en los millones de hodlrs globales de último recurso.

ADQUIRIR BITCOIN

- El bitcoin entra en el mercado cuando los mineros venden algunos de los bitcoins que reciben como recompensa, para pagar sus gastos operativos.

- Puedes adquirir bitcoin comprando en un forma de comercio entre pares, aceptándolo como pago por bienes o servicios que ofrezcas, como regalo, o minándolo. (Un último recurso no recomendado es desde un *exchange*.)

- Cuando lo recibes, técnicamente estás recibiendo las claves privadas con las que acceder a tu bitcoin.

- El bitcoin en sí nunca sale de la blockchain.

- Se puede adquirir bitcoin de forma anónima o con verificación de identidad (KYC - Know Your Customer)

- KYC está obligado por ley a cumplir con AML (leyes contra el lavado de dinero) al comprar en intercambios.

- Dado que el bitcoin es el dinero de la libertad, recomiendo encarecidamente la compra que no requiere de verificación de identidad (KYC).

- Esto preserva tu derecho a la privacidad en el futuro.

Sin verificación de identidad
[Non-KYC] >> De forma anónima

Cómo obtener bitcoin de manera anónima:
Recomendado:

1. Elige una app de billetera sólo para bitcoins.
2. Escoge un método (leer más abajo sobre esto).
3. Compra, recibe o mina bitcoin.
4. Retira ese bitcoin a tu billetera.
5. HODL- Consérvalo

- **Compra el bitcoin en Bisq o HodlHodl. Consulta bisq.wiki** para aprender a hacerlo. Dominarlo puede llevarte un poco de tiempo, pero merece mucho la pena. ¡Mantente libre de tener que identificarte!

- **Cómpralo a través de un cajero automático de bitcoin** >> asegúrate de comprobarlo antes, porque algunos de ellos exigen identificación. Otros sólo te piden el nombre y un número (puedes usar un número de teléfono temporal).

- **Compra un vale de Azteco. Visita azte.co para ver la ubicación.**

- **Gánalo por tu trabajo** ~ pide que te paguen en bitcoin. Ofrece un descuento en tu precio

- **Cómpralo en persona en un encuentro de bitcoin.**

- Mínalo. Minar desde casa se está volviendo cada vez más fácil, o puedes unirte a un pool de minería, **pero infórmate bien para poder permanecer libre de identificarte.**

KYC >> Verificación de DNI Requerida

Cómo obtener bitcoin dando tu identificación:
No recomendable:

1. Elige una app de billetera sólo para bitcoins.
2. Elige un exchange sólo para bitcoins.
3. Créate una cuenta.
4. Vincula un método de pago.
5. Cumple con los requisitos de identificación.
6. Compra bitcoin.
7. Retira ese bitcoin a tu billetera.
8. Consérvalo HODL

Ten en cuenta que, al comprar con éste método, **tus bitcoins estarán vinculados a tu identidad para siempre.**

Si eliges este método, te recomiendo que el **exchange que uses sea fiable.**

¡Asegúrate de que el exchange te permite retirar el bitcoin que adquieras a tu billetera!

Los exchange están obligados a pedirte que te identifiques, por ley.

Tomarán tu nombre completo, dirección, número de la Seguridad Social, correo electrónico, número de teléfono, y con frecuencia, una foto tuya sosteniendo tu DNI.

Verifica que el *exchange* cuente tanto con un correo electrónico como un teléfono de contacto para la atención al cliente.

Pídeles que te guíen a través del envío de tu bitcoin, desde la cuenta que has creado con ellos, hasta tu billetera para que, de esta manera, custodies tu bitcoin = **ten tus propias claves.**

- Esto NO borra el hecho de que les hayas comprado bitcoins…ni lo hará nunca.
- Las transacciones se pueden rastrear en la cadena, y en muchos países hay que pagar impuestos cuando se gasta bitcoin.

Evita comprar a través de Venmo y PayPal, ya que actualmente no puedes retirar tus sats a tu propia billetera.

Como dicen en BT (Bitcoin Twitter):

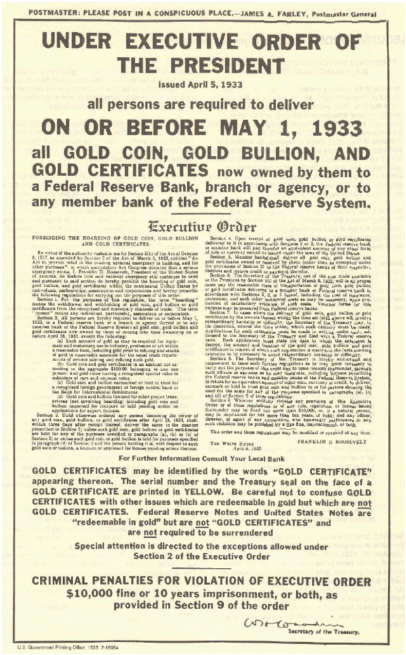
> **"Sin claves, no hay queso", o "No son tus claves, no es tu bitcoin"**

Lo que quiere decir esto es que, mientras un servicio centralizado tenga las claves privadas de tu bitcoin, sigue existiendo la posibilidad de que su plataforma sea hackeada, o que sufra una **captura regulatoria** y pierdas tu bitcoin.

Orden Ejecutiva 6102 (EO 6102)

Esto pasó con el oro en 1933. **El presidente Roosevelt emitió la Orden Ejecutiva 6102, que obligaba a todos los ciudadanos estadounidenses a entregar la mayor parte de su oro a cambio de billetes.**

El valor del oro era de 20,67 dólares por onza. Al año siguiente, el gobierno aumentó el precio del oro a 35 dólares la onza con la Ley de Reserva de Oro de 1934, devaluando de hecho los billetes que la gente había recibido en su momento, ya que el valor de sus billetes nunca subió con el precio inflado del oro.



POSTMASTER: PLEASE POST IN A CONSPICUOUS PLACE.--JAMES A. FARLEY, Postmaster General

UNDER EXECUTIVE ORDER OF THE PRESIDENT

Issued April 5, 1933

all persons are required to deliver

ON OR BEFORE MAY 1, 1933

all GOLD COIN, GOLD BULLION, AND GOLD CERTIFICATES now owned by them to a Federal Reserve Bank, branch or agency, or to any member bank of the Federal Reserve System.

Executive Order

FORBIDDING THE HOARDING OF GOLD COIN, GOLD BULLION AND GOLD CERTIFICATES.

For Further Information Consult Your Local Bank

GOLD CERTIFICATES may be identified by the words "GOLD CERTIFICATE" appearing thereon. The serial number and the Treasury seal on the face of a GOLD CERTIFICATE are printed in YELLOW. Be careful not to confuse GOLD CERTIFICATES with other issues which are redeemable in gold but which are not GOLD CERTIFICATES. Federal Reserve Notes and United States Notes are "redeemable in gold" but are not "GOLD CERTIFICATES" and are not required to be surrendered

Special attention is directed to the exceptions allowed under Section 2 of the Executive Order

CRIMINAL PENALTIES FOR VIOLATION OF EXECUTIVE ORDER
$10,000 fine or 10 years imprisonment, or both, as provided in Section 9 of the order

THE WHITE HOUSE, April 5, 1933. FRANKLIN D. ROOSEVELT

Secretary of the Treasury.

Hubo que esperar 42 años, hasta 1975, para que se derogara esta ley.

Aunque esto es poco probable, no es imposible. En este momento, no tenemos mucha idea de cómo van a responder los reguladores al bitcoin a medida que siga ganando popularidad y una adopción más generalizada.

Hasta ahora, la acogida ha sido mixta. Sin embargo, por el momento, parece que muchos entienden, o tal vez sólo aceptan, que el bitcoin no puede ser detenido en última instancia.

Hay varios políticos que empiezan a hablar en favor del bitcoin como parte de su programa. También hay algunos en contra.

En última instancia, a todos los gobiernos les convendría adoptarlo y añadirlo a sus balances como protección contra sus monedas fiduciarias, que se inflan y degradan rápidamente.

El Salvador está muy por delante de este punto, ya que convirtió al bitcoin en una moneda legal en 2021.

¡Es emocionante ver qué país será el siguiente!

ALMACENAR BITCOIN DE FORMA SEGURA

- Una vez hayas dado el paso que te ha cambiado la vida de hacer tu primera compra de ₿ (¡felicidades!), tienes que decidir cómo guardarlos de manera segura.

- **Ser tu propio banco es una poderosa forma de auto-soberanía.**

- **¡Todo lo que hace falta es tomárselo en serio!**

- ***Por favor, infórmate e investiga sobre este tema por tu cuenta antes de leer mis recomendaciones básicas***

- **El ecosistema bitcoin está evolucionando cada minuto.**

- Twitter es un buen sitio para estar al tanto de las últimas novedades (hasta que una app mejor y descentralizada gane tracción).

ECHA UN VISTAZO A ESTOS SITIOS DONDE PUEDES ENCONTRAR TUTORIALES:

- ➢ Bitcoin Sessions en You Tube
- ➢ Bitcoiner.guide
- ➢ Armantheparman.com

BILLETERAS SÓLO PARA BITCOIN (BITCOIN WALLETS)

- La mejor manera de almacenar bitcoin es en tu propia:
  - ➢ custodia propia
  - ➢ Sin custodios
  - ➢ Billetera únicamente para bitcoin

- Una "billetera" o "wallet" es en realidad una pieza de software, que es un dispositivo de firma. Contiene tus claves privadas, las cuales utiliza para firmar una transacción que envíes (broadcast).

BILLETERA CALIENTE (HOT WALLET)

- **Ésta es una aplicación online de bitcoin, que te descargas en tu móvil u ordenador.**
- Es mejor utilizarla para cantidades pequeñas, para los gastos diarios.

BILLETERA FRÍA / COLD STORAGE WALLET

- **Esta es una billetera offline.** También conocida como *hardware wallet.*
- Se trata de un dispositivo de hardware independiente en el que se guardan tus claves. Es como una caja de seguridad.

➢ **Por favor, investiga sobre ello para comparar las características y compensaciones entre las billeteras.**

Aunque ambas funcionan bien, en general se recomienda utilizar una billetera fría una vez se tienen más de entre 500 y 1000 dólares en bitcoins, ya que es más seguro.

APPS DE BILLETERAS CALIENTES / HOT WALLETS

Muun Wallet, Blue Wallet, Samourai Wallet (Android only), Sparrow Wallet, Green Wallet, Phoenix Wallet

BILLETERAS FRÍAS PARA ALMACENAMIENTO / COLD STORAGE WALLETS

Cold Card, Trezor, Passport, Keystone,
Blockstream Jade, Seed Signer, Bitbox,

Compra SIEMPRE tu billetera fría directamente del fabricante, para asegurarte de que no ha sido manipulada.

CONFIGURACIÓN DE LA BILLETERA

- **Follow BTC Sessions on YouTube** for excellent tutorials on wallet set-up (and lots more).

- Consulta BTC Sessions en YouTube para ver unos tutoriales excelentes sobre configuración de billeteras (y muchas más cosas).

- **Cuando configures tu billetera, asegúrate de tener papel a mano para escribirte la semilla, compuesta de 12 o 24 palabras.**

- **Mantenla offline. Nunca le hagas una foto.**

- **GUARDA LA SEMILLA EN LUGAR SEGURO. MUY, PERO QUE MUY SEGURO!**

- **Muchas empresas fabrican placas metálicas en las que se pueden perforar las palabras de la semilla para una mayor protección contra el fuego y el agua.**

- Si perdieras el acceso a tu billetera (tanto caliente como fría) puedes restablecerlas con esta semilla y recuperar tus fondos.

- Puedes hacerlo en cualquier billetera que admita el mismo tipo de semilla BIP39 (12/24 palabras).

- La mejor práctica sería almacenar la **ruta de derivación** de tu billetera, además de tu semilla.

- **Recuerda: ¡Cualquiera que tenga la semilla tiene acceso a tu bitcoin!**

SOBRE LA PRIVACIDAD

La privacidad se está volviendo cada vez más importante a la hora de comprar (de forma anónima), **asegurar, almacenar y gastar bitcoins,** especialmente a la luz de los recientes eventos con cuentas bancarias incautadas/congeladas.

Además, **la privacidad digital general es fundamental si deseas obtener soberanía online y protegerte de la vigilancia indebida y el fraude.**

A continuación puedes ver algunos servicios actuales centrados en la privacidad. Está más allá del alcance de este libro profundizar en cada uno de ellos, así que busca información por tu cuenta, sigue las cuentas de Twitter que menciono a continuación para estar al tanto de nuevas actualizaciones.

> La privacidad es necesaria para una sociedad abierta en la era electrónica. La privacidad no es un secreto. Un asunto privado es algo que uno no quiere que todo el mundo sepa, pero un asunto secreto es algo que uno no quiere que nadie sepa. La privacidad es el poder de revelarse selectivamente al mundo.
>
> ~Eric Hughes, From 'A Cypherpunk's Manifesto'

GUÍAS DE PRIVACIDAD

- **Bitcoiner.guide** @BitcoinQ_A
- Econoalchemist.com @econoalchemist
- Sethforprivacy.com @sethforprivacy
- diverter.hostyourown.tools @Diverter_NoKYC
- Citadeldispatch.com @ODELL
- KYCnot.me
- Lopp.net @lopp > Click Resources > Privacy
- Privacytools.io
- Enegnei.github.io
- Restoreprivacy.com @ResPrivacy
- Keepitsimplebitcoin.com @KISBitcoin
- @SovrnBitcoiner
- K3tan.com @_k3tan

VPN (Virtual Private Network para ocultar tu ISP)

- Mullvad.net - Paga con bitcoin

APLICACIONES DE AUTENTICACIÓN EN DOS FACTORES

- Authy
- Google Authenticator
- Yubi Key

NAVEGADORES CENTRADOS EN LA PRIVACIDAD

- TOR
- Firefox
- Brave

APLICACIÓN DE "NOTAS" ENCRIPTADAS:

- StandardNotes.com

BUSCADORES CENTRADOS EN LA PRIVACIDAD

- Duck Duck Go
- Brave
- Startpage
- Qwant

APLICACIONES DE MENSAJERÍA CENTRADAS EN LA PRIVACIDAD

- Signal
- Session
- Element

EJECUTAR TU PROPIO NODO

- Bitcoin Core
- Ronin Dojo
- Run Citadel
- Raspi Blitz
- Umbrel - Si solo ejecuta su nodo bitcoin en él..

SERVICIOS DE MEZCLA

- Coinjoin
- Paymarket
- Coinswap

TELÉFONOS MÓVILES / TELÉFONOS DE UN SOLO USO

- Run Calyx OS en un Android Pixel
- Text Verified

GASTOS PRIVADOS

- Pay with Moon
- Bitrefill
- Paxful

PRIVATE RECEIVING ADDRESS BOT

- PayNym

REDES SOCIALES DESCENTRALIZADAS

- Mastodon
- Zion (tarifa mensual, se agregará bitcoin como opción de pago)

La posibilidad de ser anónimo o seudónimo depende de que no reveles ninguna información de identificación tuya en relación con las direcciones de bitcoin que utilizas. Si publicas tu dirección de bitcoin en la web, entonces estás asociando esa dirección y cualquier transacción bajo el nombre con que la publicaste.

Si has publicado bajo un identificador que no has asociado con tu identidad real, entonces todavía eres seudónimo.

~ Satoshi Nakamoto, 25-11-2009

Para una mayor privacidad, es mejor utilizar las direcciones de bitcoin una sola vez. Puedes cambiar la dirección tan a menudo como quieras.

~ Satoshi Nakamoto, 25-11-2009

DISIPANDO bitcoin FUD*

(Fear Uncertainty Doubt. Miedo, incertidumbre, duda)

- A continuación se exponen algunas discusiones o miedos comunes sobre bitcoin.
- Son, en gran parte, infundadas, resultado de la ignorancia, o tal vez de una completa incomprensión
- Aquí ofrezco breves refutaciones a cada una de ellas, y al final encontrarás referencias a recursos que profundizan más y refutan todos estos miedos, incertidumbre y dudas.

BITCOIN USA DEMASIADA ENERGÍA

> *El calor de tu ordenador no se desperdicia si necesitas calentar tu casa…El coste es igual si generas el calor con tu ordenador.*
>
> *~ Satoshi Nakamoto, 9-8-2010*

> *Al principio, la producción de mercancía parece un desperdicio simplemente porque es costosa. Sin embargo y, sin olvidar su alto coste, la materia prima agrega valor repetidamente, al permitir transferencias de riqueza que resultan beneficiosas. Una gran parte del coste se recupera cada vez que se hace posible o se abarata una transacción. Ese coste, que inicialmente era un total desperdicio, se amortiza en muchas transacciones.**
>
> ~ Nick Szabo
> Cypherpunk

- **"Demasiada" energía es una propuesta de valor que debe tener en cuenta cómo valoramos la finalidad del uso de la energía.***
- **Si tenemos en cuenta que las luces de navidad de EE.UU consumen tanta electricidad como toda la red Bitcoin, quizá veamos que todo es relativo.**
- Usar energía, incluso una gran cantidad de ella, para asegurar el dinero más duro y resistente a la censura que la humanidad haya conocido jamás, ¡merece la pena al 1000%!
- Al comparar el consumo de energía de bitcoin con el del sistema tradicional, también debemos tener en cuenta la "montaña completa" de ambas partes:

Ecosistema Bitcoin	Legado del sistema Fiat
Mineros ASIC* (Circuito Integrado para Aplicaciones Específicas)	BIS (Banco de Pagos Internacionales)
Nodos	Bancos Centrales
Hardware Wallets	Bancos Nacionales / Regionales
Apps de Software Wallet	Complejo militar industrial
	Copias de seguridad de los bancos
	Impresión física de dinero
	Apps de bancos online
	Red de cajeros automáticos

- Al utilizar bitcoin, reduciremos en última instancia el consumo de energía en multitud de otros ámbitos, sobre todo al dejar de necesitar el complejo industrial militar para proteger el petrodólar.

> *Bitcoin es un derecho de propiedad independiente del monopolio de la violencia.*
> ~ @breedlove

- Además, el consumismo desenfrenado que se requiere para mantener a flote el sistema basado en la deuda se reducirá con el tiempo, ya que **el dinero duro incentiva el gasto prudente y el ahorro de forma natural** (ya que tus ahorros realmente mantendrán su valor, un concepto que no hemos experimentado desde que salimos del patrón oro).

- **Por último, y lo que es muy importante, la minería de bitcoins ya está reduciendo la contaminación al capturar el gas natural quemado y utilizarlo para alimentar a los mineros.** Dado que los mineros buscan bajos costes de electricidad, también es probable que sea el mayor impulsor hacia la energía renovable de bajo coste, ya que los incentivos coinciden.

- Nic Carter, Troy Cross, NYDIG, el vídeo "This Machine Greens" de Swan Bitcoin en YouTube y un excelente episodio del programa "What is Money" (WiM161) con B.Quittem **incluyen información muy detallada** sobre Bitcoin y la energía.

BITCOIN ES UN PONZI (ESTAFA PIRAMIDAL)

Bitcoin no es un ponzi (estafa piramidal):

- Los nuevos inversores no pagan nada a los antiguos.
- Al comprar bitcoin, nadie promete una **devolución** de esa inversión.
- No hay liderazgo ni **equipo de promociones.**
- No hubo una **mina previa.**
- **Lee** "Why Bitcoin is not a Ponzi" de Lyn Aiden para saber más.

BITCOIN ES DEMASIADO LENTO

Mientras que la base de Bitcoin es lenta, **la segunda capa (Red Lightning) construida sobre la capa base es…¡rápida como un rayo!**

La red de Bitcoin puede procesar alrededor de 7 transacciones por segundo (TPS).

La red Visa afirma que puede procesar hasta 24.000 TPS, aunque 4.000 TPS se aproximan más a la cifra real.

La red Lightning, una solución de segunda capa construida sobre Bitcoin, ¡tiene capacidad para procesar millones de transacciones por segundo!*

LOS GOBIERNOS PODRÍAN PROHIBIR EL BITCOIN

- Algunos gobiernos lo han intentado, como los de China, India y Nigeria. En cada caso, el uso de bitcoin aumenta* rápidamente entre la población de dichos países.

- No hay forma de que los gobiernos "prohíban" realmente el bitcoin, ya que por su naturaleza **no necesita permiso, y es resistente a la censura.* Es código, y el código es expresión.**

- Dicho esto, los gobiernos pueden dificultar la compra y venta con dinero fiat. También pueden gravarlo como una mercancía, como hacen en EE.UU.

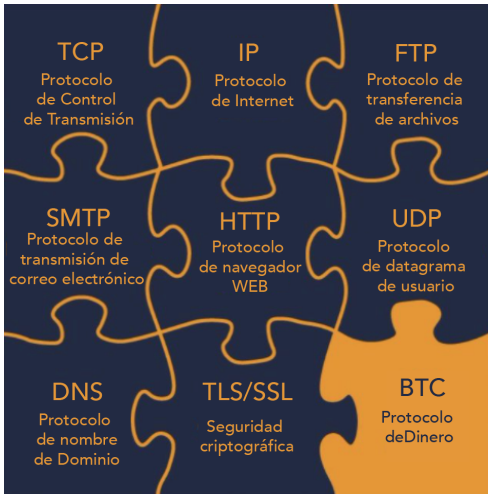
- En última instancia, no les favorecerá el intentar prohibirlo, ya que bitcoin es algo inevitable y están empezando a verlo. **Serían mucho más inteligentes si lo añadieran al balance de su país como cobertura frente a la inflación de sus monedas fiat.***

> *A los gobiernos se les da bien cortar las cabezas de una red con control centralizado como Napster, pero las redes P2P (entre pares) puras como Gnutella y Tor parecen estar resistiendo.*
>
> *~ Satoshi Nakamoto*

- **Un gran artículo:** Can Government Stop Bitcoin? De Alex Gladstein, Director de Estrategia de la Fundación de los Derechos Humanos.

BITCOIN ES TECNOLOGÍA ANTIGUA

- **Más bien es "tecnología definitiva"** en lo que respecta a la escasez digital, la descentralización y la resolución tanto del problema del doble gasto como el problema de los generales bizantinos. Una vez descubierta, no se puede volver a descubrir.
- **Una vez inventada la rueda, ésta no podía volver a ser inventada.**
- El protocolo TCP/IP con el que funciona internet, ha sido el estándar para todas las redes informáticas desde 1983. Es probable que siga siéndolo durante mucho tiempo.
- Una vez descubierta una tecnología de capa base que funcione óptimamente, puede durar cientos o miles de años.



Credit: @DecouvreBitcoin

BITCOIN LO USAN LOS CRIMINALES

- **También lo es el dólar, y cualquier otra moneda fiat del mundo.** Aunque estas actividades me entristecen enormemente, es simplemente incorrecto atribuirlas al bitcoin en sí. **Bitcoin es una herramienta, al igual que un cuchillo, y depende de cada uno de nosotros el uso que le demos.**

- Nota: Dado que la blockchain de Bitcoin es auditable, la verdad es que es una mala elección para la actividad criminal.

LA COMPUTACIÓN CUÁNTICA PODRÍA ACABAR CON BITCOIN

- Aunque es posible que esto ocurra en un futuro, los **desarrolladores están trabajando en soluciones de cifrado post-cuántico.** Dichas soluciones se aplicarían cuando fuera necesario.

- Bitcoin es sólo una de las muchas aplicaciones online que confían en el hash SHA-256 para su seguridad. Incluso los militares lo utilizan, por lo que existe un gran incentivo más allá de la comunidad bitcoin para desarrollar nuevos protocolos de cifrado.

- Además, si el SHA-256 llega a su fin, tendremos mucho más de lo que preocuparnos además del bitcoin.

BITCOIN NO TIENE VALOR REAL

"El valor de los bitcoins se debe a su escasez"
~ Fidelity Digital Assets

- **Rareza es valor. Todo el dinero a lo largo de la historia se ha valorado porque tenía cierto grado de escasez.**

- Además, estaba respaldado por la creencia de que mantendría su valor, de modo que podría intercambiarse en el futuro por otra cosa que fuera de valor.

- A medida que crece la red Bitcoin, respaldada por las propiedades monetarias superiores que encarna, el efecto de red crece exponencialmente.*

- Cuanto mayor es el efecto de red, más valor ofrece, como bien escaso. El valor es un reflejo de la demanda, y a medida que ésta aumenta, aumenta también el valor.

ALGUNAS PERSONAS TIENEN DEMASIADO

- Es cierto que algunas personas tienen mucho más que otras. **Al liberar el protocolo, Satoshi permitió al bitcoin circular libremente, y aquellos que comprendieron el potencial que encerraba, lo minaron o compraron antes. Era la forma más justa y orgánica posible de presentarlo al mundo.**

- Con el tiempo, cuando el mundo se "hiperbitcoinice", es decir, cuando vivamos en un estándar bitcoin, aquellos que tengan más lo gastaran de forma natural en la economía.*

- Aunque en cierto momento ya no se podrá comprar con dinero fiat, la gente cobrará por su trabajo en bitcoin. Recibir dinero sólido de verdad nos permitirá tener ahorros reales que no se degradarán con el tiempo por la inflación.

- Aunque siempre habrá quien tenga más riqueza y quien tenga menos, debido a un gran número de factores, **un estándar bitcoin hará permeable la membrana entre las distintas clases de riqueza,** como dice Aleks Svetsi. Esto permitirá que la movilidad ascendente y descendente sea mucho, mucho más fluida de lo que es hoy.

- **Habiendo nacido y nadado toda nuestra vida en un mundo de dinero fiat, ¡es casi imposible imaginar y comprender las implicaciones de tener un dinero que no pueda ser degradado o manipulado!.**

BITCOIN ES DEMASIADO VOLÁTIL

- **Esto es algo normal durante la fase de descubrimiento de un nuevo activo monetario.** No hay otra forma de que se produzca crecimiento cuando es orgánico y emergente (en lugar de descendente y ordenado).

- Además, en esta etapa de la existencia humana, con cambios exponenciales en todas las esferas, es lógico que algo tan revolucionario como el bitcoin sufra cambios tan brutales.

- Aunque los que estamos dentro de la madriguera de conejo lo vemos como el futuro, actualmente sólo el 1-2% de la población mundial tiene bitcoins. Esto hace que sea vulnerable a una gran volatilidad.

- A medida que madure y aumente su **adopción**, dicha volatilidad disminuirá y, finalmente, se estabilizará y convertirá en una **unidad de cuenta**.

> *Estoy seguro de que dentro de 20 años habrá un gran volumen de transacciones, o no habrá volumen.*
>
> ~ Satoshi Nakamoto 2010-02-14

BITCOIN NO ES TANGIBLE

- **Esto se trata de una característica, no es un error.** El hecho de que bitcoin no sea físico es uno de los principales factores que contribuyen a que no se pueda confiscar.

BITCOIN PODRÍA SER HACKEADO

- Desde que se lanzó, hace 14 años, nunca ha sido hackeada.
- Sin embargo, sí se han producido hackeos en los intercambios, por lo que recomiendo encarecidamente trasladar tus bitcoins a tu propia billetera de auto-custodia lo antes posible.
- Se calcula que para descifrar el cifrado SHA-256 (que utiliza bitcoin) en 24 horas, un ordenador cuántico necesitaría 13 millones de qubits físicos. Actualmente, el récord de qubits en poder de IBM es de tan sólo 127.
- Se da por sentado que se desarrollará un método de cifrado seguro desde el punto de vista cuántico mucho antes de que sea necesario.

> *Ser de código abierto significa que cualquiera puede revisar el código de forma independiente. Si fuera de código cerrado, nadie podría verificar la seguridad. Creo que es esencial que un programa de esta naturaleza sea de código abierto.*
>
> *~ Satoshi Nakamoto, 10-12-2009*

PUEDES DESPEJAR MÁS DUDAS AQUÍ:

- Endthefud.org
- Bitcoinmythbusters.org
- Casebitcoin.com
- Safehodl.github.io/failure/
- Lopp.net - Misconceptions

Bitcoin es fundamentalmente diferente de cualquier otro activo digital. Es probable que ningún otro activo digital mejore a bitcoin como activo monetario, porque bitcoin es el dinero digital más seguro, descentralizado y sólido (en comparación con otros activos digitales) y cualquier "mejora" necesariamente tendrá que enfrentar compensaciones.

Informe de Fidelity Digital Assets, "Bitcoin First", Enero de 2022
Chris Kuiper, Analista Financiero Certificado, Director de Investigación
Jack Neureuter, Analista de Investigación

- **Para mí, tener bitcoins (hodling) es como tener una inversión a largo plazo**

- El precio diario no importa, ya que se espera que sea volátil (que suba y baje) durante algunos años todavía..

- Como he mencionado anteriormente, esto es algo normal para un nuevo activo en proceso de descubrimiento de precios.

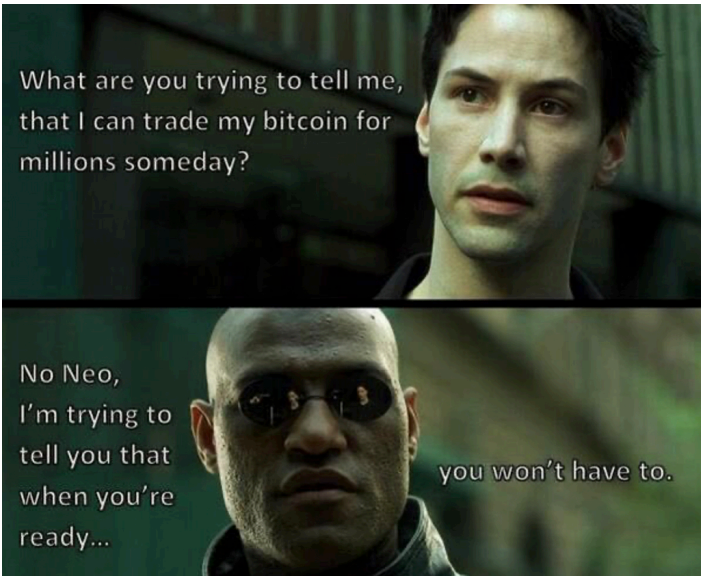
- Si uno amplía el gráfico de precios BTC/USD, verá que ha aumentado un +31,296% desde 2009, con un promedio del 200% por año.

- Las oscilaciones del precio reflejan diversos artículos de prensa, actualizaciones normativas, demanda del mercado, miedo y emoción. ¡Es una montaña rusa!

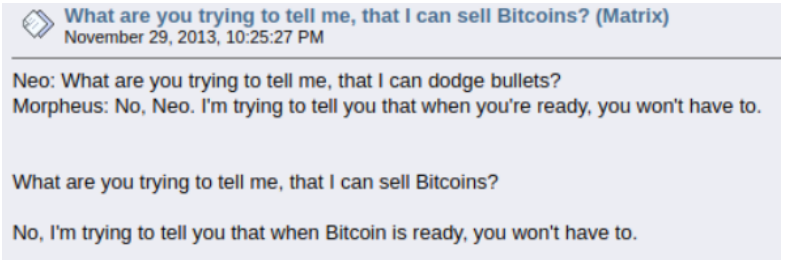
- **Cuanto más tiempo se invierte, más se aprenden y entienden los fundamentos, y más se comprenden las profundas implicaciones de tener un dinero sólido, menos importa el precio.**

- **Al final, "el precio", no importará en absoluto, ya que el bitcoin será la unidad de cuenta.**

- Dicho esto, debo añadir esta advertencia: el consejo general es invertir sólo lo que uno "pueda permitirse perder", ya que, por supuesto, no hay garantías.



Neo: que me querías decir? que puedo hacer millones trading con bitcoin?
Morpheus: No Neo, lo que intento decirte es cuando estes listo no tendrás que hacerlo.
-El Matrix.



Neo: que me querías decir? que puedo esquivar las balas?
Morpheus: No Neo, lo que intento decirte es cuando estes listo no tendrás que hacerlo
-El Matrix.

Original bitcointalkforum.org source for one of the most classic bitcoin memes of all time.

MIENTRAS TANTO, HABLEMOS DE LOS IMPUESTOS…

>> Descargo de responsabilidad: ¡Esto no es asesoramiento financiero ni fiscal!

- En el código fiscal de EE.UU, el bitcoin está considerado actualmente como una mercancía, por lo que puede tener implicaciones fiscales si lo vendes de nuevo en fiat, o incluso si compras algo con tu bitcoin.
- Si el precio bajó antes de que lo vendieras o gastaras, puedes reclamar una pérdida.
- Si el precio ha subido, se supone que debes reclamar una plusvalía y pagar entre un 10 y un 30% de CGT (Capital Gains Tax - Impuesto sobre plusvalías)
- La cuantía depende de varios factores, como el tiempo que lo hayas tenido antes de venderlo o gastarlo, y en qué tramo de IRPF te encuentres.
- Si tienes pensado vender o gastar bitcoin, especialmente grandes cantidades, puedes considerar consultar con un asesor fiscal.
- Si simplemente lo compras y almacenas, actualmente no **cuentas** con ningún hecho sujeto a impuestos con respecto a bitcoin.
- Y sin compras sin tener que identificarte…

¿POR QUÉ SÓLO bitcoin?

De las más de 20.000 (¡exacto, 20.000!), criptomonedas que existen, **bitcoin es el único** que es:

- **REALMENTE descentralizado**
- Con un libro de contabilidad **REALMENTE** distribuido
- Un suministro **REALMENTE** duro
- Un libro de contabilidad **REALMENTE** inmutable
- Un **efecto de red** creado a lo largo de 14 años
- ¡Y una política monetaria con la que no se puede jugar!

- **Todas las demás criptomonedas cuentan con un grupo pequeño y centralizado que controla la oferta y/o tiene el poder de cambiar el protocolo de la capa base (política monetaria).**

- **Esto es igual que el sistema bancario central fiat que vemos hoy en día.**

- Un poder centralizado como éste se presta a la manipulación y la corrupción.

- Véase la estafa pump/dump (bombeo y descarga) de altcoin descrita en la página siguiente..

- También:
- Podcast de Stephan Livera con Guy Swann (SLP306)
- Una lista de rug-pulls de altcoin/defi: https://rekt.news/leaderboard

ESTAFAS PUMP AND DUMP DE ALTCOIN

➢ Por desgracia, estos casos son reales, y ocurren a diario con tokens distintos al bitcoin.

➢ Existen varias **iteraciones**, pero uno de los tipos más comunes es el siguiente:

Creación del token: Se crea una nueva criptomoneda (¡es mucho más fácil de lo que parece!)

Website: A menudo, se crea un sitio web que llame la atención para que ésta parezca legítima.

Influencers pagados: Se promocionan en redes sociales.

Grupos de información privilegiada de pago: La información se envía a líderes de algunos de los cientos de grupos de "comercio" o "inversión", donde la gente paga cuotas mensuales o anuales para obtener "información privilegiada".

Pre-Lanzamiento: Los influencers y los líderes de grupos de pago compran primero, al precio más bajo.

Lanzamiento: La moneda es "lanzada" por estos influencers y líderes, que dicen a sus seguidores "¡Rápido, comprad ahora!"

Pump: Los precios suben rápidamente porque sus seguidores se dan prisa en entrar cuanto antes.

El rápido aumento de precios atrae a la gente normal a comprar con la esperanza de hacer fortuna.

- Lo que, a su vez, hace subir aún más el precio.

- **Dump:** Esta es la parte triste; suele ocurrir rápidamente. En un momento dado, los jefes de grupo que fueron pagados venden sus tokens, "en lo más alto". Luego, dicen a sus seguidores que vendan.

- Debido a que mucha gente vende al mismo tiempo, y la liquidez suele ser baja al tratarse de una moneda nueva, el precio baja rápidamente.

- **Pánico:** La caída del precio provoca pánico entre el público en general, que no tiene ni idea de estos chanchullos, y empiezan a vender en pánico.

- **Bag-Holders:** El final de esta triste historia es que los que se quedan "aguantando la bolsa" probablemente la tendrán para siempre.

- Sin ningún valor real ni fundamentos, la mayoría de estos tokens nunca recuperan un precio de mercado.

SEGURIDAD Y CÓMO EVITAR ESTAFAS

- **Cíñete al bitcoin.**
- **¡Presta mucha atención** a tu ciberseguridad!
- **Investiga por tu cuenta y asegura tu bitcoin** con sumo cuidado.
- **¡NUNCA le des las palabras de tu semilla a nadie a quien no le darías la llave que contiene todo tu oro!**
- **NUNCA hagas click en ningún enlace** de tu correo electrónico que te pida confirmar datos de cuenta de ningún tipo. En su lugar, **ve directamente al sitio web oficial** y comprueba si tienes alguna notificación que requiera alguna acción.
- **TEN EN CUENTA** que hay un sinfín de cuentas falsas que imitan a otras con muchos seguidores en las redes sociales. Si un influencer te envía un MD sin más, probablemente se trate de una estafa.
- EVITA todas las estafas que aparecen en las redes sociales prometiendo duplicar tu bitcoin si les envías algo. ¡Eso no va a suceder!
- EVITA esas mismas estafas sobre **"duplicar tu bitcoin"** en YouTube.
- **ASEGÚRATE** de que la dirección a la que envías tu bitcoin es la correcta, ya que las transacciones son irreversibles.

LOS NÚMEROS DE SATOSHI

3-6-9

Bitcoin está diseñado para minar 6 bloques por hora >> un bloque por cada ~ 10 minutos

- 24 horas en un día:
  2+4=6

- Es decir, 144 bloques al día:
  1+4+4=9

- 52560 bloques al año:
  5+2+5+6+0=18
  1+8=9

- 52704 bloques por año bisiesto:
  5+2+7+0+4=18
  1+8=9

- 21 millones de monedas:
  2 + 1 + 0 + 0 + 0 + 0 + 0 + 0 = 3

- 33 Halvings: (mitades)
  3 + 3 = 6

- La dificultad se ajusta cada 2016 bloques:
  2 + 0 + 1 + 6 = 9

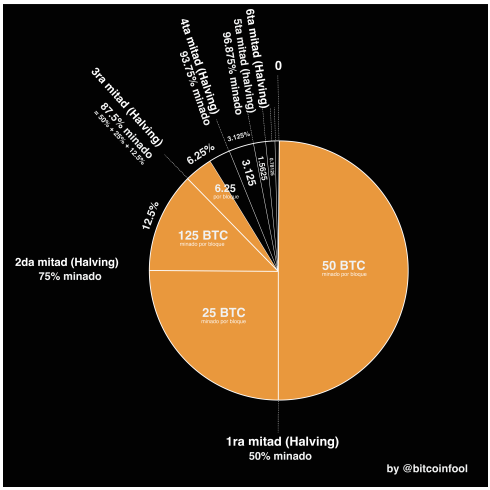
~ Basado en un tweet de @level39

- La recompensa por bloque se reduce a la mitad cada 210,000th bloques (cada cuatro años)
  2 + 1 + 0 + 0 + 0 + 0 = 3

Si supieras la magnificencia de los números 3, 6 y 9,
tendrías la llave del universo
~ Nikola Tesla

RECOMPENSA POR BLOQUE = % DEL SUMINISTRO

- La recompensa por bloque (número de bitcoins recompensados por cada nuevo bloque minado) representa el porcentaje del suministro total que se minará durante esa época.
- Por ejemplo, la recompensa por bloque actual (2020-2024) es de 6,25 bitcoin.
- En estos mismos cuatro años, se minará el 6,25% de los 21 millones de bitcoin que hay.
- Satoshi, ¡no dejas de sorprender!



Credit: @bitcoinfool

PICOS DE RECOMPENSA

Cada cuatro años, las recompensas de bitcoin se reducen a la mitad por cada bloque extraído. Una Época de Recompensa es ese período de cuatro años.

Pico 1: 2009-2012
= (50 bitcoin * 210,000 bloques) = 10,500,000 bitcoins
1+0+5+0+0+0+0+0 = 6

Pico 2: 2012-2016
= (25 * 210,000) = 5,250,000 bitcoins
5+2+5+0+0+0+0 = 12
1+2 = 3

Pico 3: 2016-2020
= (12.5 * 210,000) = 2,625,000 bitcoins
2+6+2+5+0+0+0 = 15
1+5 = 6

Pico 4: 2020-2024
= (6.25 * 210,000) = 1,312,500 bitcoins
1+3+1+2+5+0+0 = 12
1+2 = 3

Pico 5: 2024-2028
= (3.125 * 210,000) = 656,250 bitcoins
6+5+6+2+5+0 = 24
2+4 = 6

Pico 6: 2028-2032
= (1.5625 * 210,000) = 328,125 bitcoins
3+2+8+1+2+5 = 21
2+1 = 3

Pico 7: 2032-2036
= (0.78125*210,000) = 164,062.5 bitcoins
1+6+4+0+6+2+5 = 24
2+4 = 6

EL CUMPLEAÑOS DE SATOSHI

- **El 5 de Abril de 1975** es la fecha que Satoshi proclamó como su cumpleaños.
- Aunque no podemos saber si ésta fue realmente su verdadera fecha de nacimiento, es muy interesante.
- **El 5 de Abril (de 1993)** fue el día en que el Presidente de EE.UU, Franklin D. Roosevelt, firmó la Orden Ejecutiva 6102, "prohibiendo el atesoramiento de monedas, lingotes y certificados de oro dentro de los Estados Unidos continentales".
- **1975** fue el año en que finalmente se derogó la Orden Ejecutiva 6102, y los ciudadanos estadounidenses volvieron a poder poseer más de 5 onzas de oro, más de 4 décadas después.

UN PALÍNDROMO, 6102 - 2016

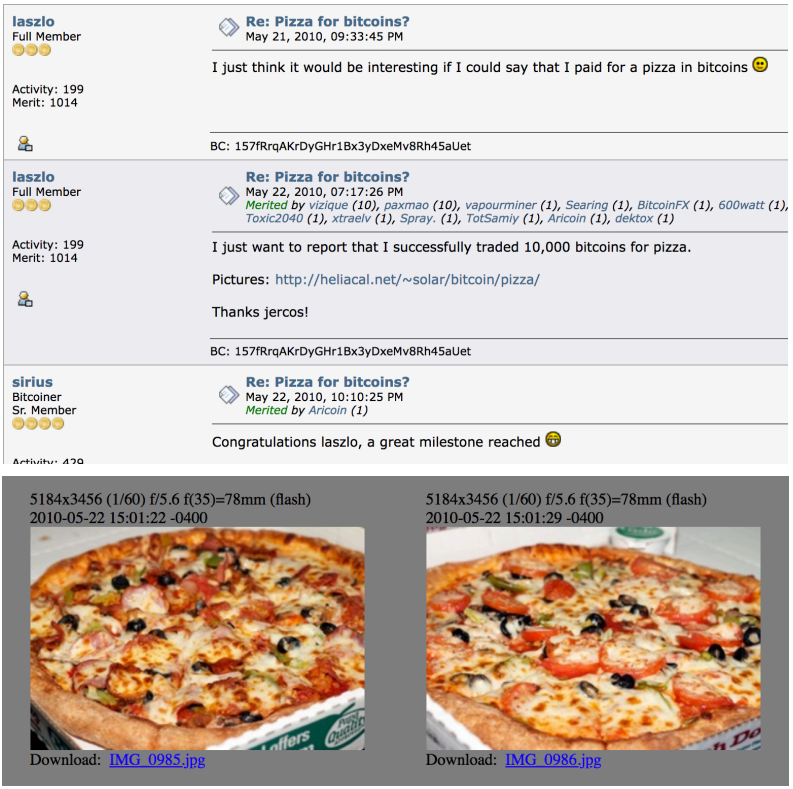
- **6102** era el número de la citada Orden Ejecutiva.
- **2016** es el número de bloques minados durante cada ajuste de dificultad (2 semanas, aproximadamente).

➢ En los dos ejemplos anteriores, se podría plantear que Satoshi utilizaba los números para indicar una inversión, una reversión del daño infligido por la extralimitación gubernamental.

- El 22 de Mayo es conocido como el Bitcoin Pizza Day. ¡Fue el día que Laszlo Hanyecz anunció en bitcointalkforum.org que había canjeado 10.000 bitcoins por dos pizzas! Por aquel entonces, eso eran unos 40 dólares. traded 10,000 bitcoin for pizza! Back then it was about $40.

- Al precio de hoy, eso serían unos 420,000.000 de dólares :) ☺

- Fue un hito para bitcoin, ya que fue el primer caso conocido de alguien que intercambiaba bitcoin por un bien o servicio. ¡Qué camino tan largo hemos recorrido!



FECHAS SEÑALADAS DEL CALENDARIO BITCOIN

18-8-2008: Se registró el dominio bitcoin.org (1+8+8+2+0+0+8 = 27, 2+7 = 9)

31-10-2008: **Bitcoin White Paper Day:** El White Paper, titulado "Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario", fue publicado por un criptógrafo anónimo llamado Satoshi Nakamoto en la lista de correo de criptografía en metzdowd .com (3+1+1+0+2+0+0+8 = 15, 1+5 = 6)

3-1-2009: **Cumpleaños de Bitcoin:** La red Bitcoin fue lanzada, cuando Satoshi minó el bloque Génesis. (3+1+2+0+0+9 = 15, 1+5 = 6)

12-1-2009: Tuvo lugar la primera transacción de bitcoins, cuando Hal Finney recibió diez bitcoins de Satoshi. (1+2+1+2+0+0+9 = 15, 1+5 = 6)

October 5, 2009 ~ Bitcoin has a market price for the first time, of $0.001 per coin.

22-5-2010: **Bitcoin Pizza Day:** La primera vez que se utilizó bitcoin para adquirir un bien o servicio fue cuando Lazslo Hayecz pagó ¡10.000 bitcoins por dos pizzas de Papa John's! (2+2+5+2+0+1+0 = 12, 1+2 = 3)

12-12-2010: La última vez confirmada en la que Satoshi escribió en el foro bitcointalk.org. (1+2+1+2+2+0+1+0 = 9)

8 de Febrero de 2011: Bitcoin alcanza por primera vez la paridad con el dólar estadounidense.

3 de Marzo de 2017: Bitcoin alcanza la paridad con la onza de oro.

21 de Agosto de 2021: Primer día anual del Infinito Bitcoin sugerido por el meme de Knut Svanholm.

Todo dividido entre 21 millones $\frac{\infty}{21{,}000{,}000}$

2021-09-07 ~ El Salvador becomes the first country to 7-9-2021: El Salvador se convierte en el primer país en dar curso legal al bitcoin. (7+9+2+0+2+1 = 21, 2+1 = 3)

Y eso sólo era el comienzo…

¡Aquí hay más!

RECURSOS PARA LA MADRIGUERA DE CONEJO DE bitcoin

«¡Curioso y más que curioso! dijo Alicia

PELÍCULAS

Puedes encontrarlas en YouTube:

PELÍCULAS SOBRE BITCOIN

- The Great Reset and the Rise of Bitcoin (2022)
- Where Did Bitcoin Come From (2021)
- This Machine Greens (2021) Sobre Bitcoin y Energía
- Bit X Bit: In Bitcoin We Trust (2018)
- Bitcoin Big Bang (2018) Sobre el hackeo de Mt Fox en 2014
- Magic Money: The Bitcoin Revolution (2017)
- Banking on Bitcoin (2016)
- Deep Web (2015) About Silk Road & Ross Ulbricht
- The Bitcoin Gospel (2015)
- Bitcoin: The End of Money as We Know It (2015)
- The Rise and Rise of Bitcoin (2014)
- Bitcoin in Uganda (2014)

PELÍCULAS SOBRE EL SISTEMA FIAT:

- How is Money Created (2020)
- Hidden Secrets of Money Series - Mike Maloney (Minutos 13-18)
- Who Controls All of our Money (2017)
- How the Economic Machine Works - Ray Dalio (2013)
- Inside Job (2010) - Sobre los acontecimientos que condujeron a la crisis de 2008
- The Money Masters (1996)

LIBROS:

Sobre Bitcoin:

- **Layered Money** de Nik Batia
- **21 Lessons** de DerGigi
- **The Bullish Case for Bitcoin** de Vijay Boyapati
- **The Bitcoin Standard** de Saifedean Ammous
- **Bitcoin Clarity** de Kiara Bickers
- **Inventing Bitcoin** de Yan Pritzker
- **Independence Reimagined & Bitcoin: Sovereignty Through Mathematics** de Knut Svanholm
- **Check Your Financial Privilege** de Alex Gladstein
- **Hard Money You Can't F*ck With** de Jason A.Williams
- **Why Buy Bitcoin** de Andy Edstrom
- **Bitcoin Audible:** Si prefieres escuchar a leer, Guy Swann lee libros y artículos sobre Bitcoin.

SOBRE EL ACTUAL SISTEMA MONETARIO BASADO EN LA DEUDA FIAT:

- **The Price of Tomorrow** de Jeff Booth
- **The Sovereign Individual** de JD Davidson y Lord W Rees-Mogg (no sólo sobre dinero)

PODCASTS

¡Éscuchalos en la app de Fountain para hacer stream a los hosts! Si no usas Fountain, puedes hacerlo a través de iTunes y Spotify

- **Citadel Dispatch** con Matt Odell
- **BitBuyBit Podcast** con Max Buybit
- **Bitcoin Rapid Fire** con John Vallis
- **The 'What is Money' Show** con Robert Breedlove
- **Stephan Livera Podcast**
- **This is Bitcoin Podcast** con Bitcoin Gandalf
- **Wake Up Podcast** con Aleks Svetski
- **Coin Stories** con Nat Brunell
- **The Bitcoin Standard Podcast** con Dr S. Ammous

- **Bitcoin Magazine Podcast**
- **The Bitcoin Matrix** con Cedric Youngelman
- **Bitcoin Fixes This** con Jimmy Song
- **Orange Pill Podcast** con Max Keiser and Stacy Herbert
- **What Bitcoin Did** con Peter McCormack
- **Bitcoin Audible** con Guy Swann reading books/articles

CURSOS GRATUITOS

- **Saylor Academy** - Bitcoin para Todos: Curso gratis
- **Looking Glass Education** - Cursos sobre Dinero y Bitcoin
- **Bitcoin Magazine** - 21 días de lecciones diarias sobre Bitcoin

SITIOS WEB

Cada uno de ellos tiene una gran recopilación de recursos:

- Nakamotoinstitute.org
- Bitcoinmagazine.com
- Bitcoin-only.com
- Bitcoin Wiki - En.bitcoin.it
- Lopp.net
- Casebitcoin.com
- Bitcoiner.guide
- Bitcoin.tv
- Learnmeabitcoin.com - ¡Explicación sencilla y genial sobre tecnología Bitcoin!
- Hope.com
- Bitcoin-resources.com
- Myfirstbitcoin.io (También disponible en español)

El corazón de Bitcoin:

- github.com/bitcoin

CAJEROS BITCOIN

- **Coin ATM Finder** - coinatmfinder.com
- **Coin Radar** - coinatmradar.com

ARTÍCULOS

- Bitcoinmagazine.com - ¡Nuevos y excelentes artículos cada día!
- SatoshisJournal. com - ¡Educación, noticias e historias sobre Bitcoin!
- Muchas de las cuentas de Twitter mencionadas a continuación escriben en Medium, Substack.

BT ~ BITCOIN TWITTER

Algunos cypherpunks, genios y cabralocas que puedes seguir!

A través de estas cuentas, encontrarás miles de pensadores; todos ellos están en el mismo barco.

BT es, en gran medida, donde este experimento está creciendo, desplegándose en tiempo real, a través del tiempo y el espacio, en los éteres del ciberespacio, conectado a lo físico, a través de todos nosotros, los humanos, compartiendo una visión.

Luego están los más callados, los desarrolladores que trabajan entre bastidores sin los cuales nada de esto sería posible.

Todos nosotros juntos desencadenamos, al igual que el bitcoin lo hizo sobre nosotros,

una bendición sin medidasharing a vision.

LOS TEMAS INCLUYEN: Bitcoin Proof-of-Work, Privacidad, Filosofía, Historia Monetaria, Código, Minería Bitcoin, Sociología, Teoría de Juegos, Economía Austriaca, Educación Bitcoin, Lightning Network, Entorno/Ambiente Regulatorio, Uso Energético de Bitcoin, Core Devs, Comunidades Bitcoin, Futuro de Bitcoin.

Quedas advertido: En Twitter, es de gran ayuda que no te importe que te critiquen y/o insulten; hay gente muy apasionada en defensa del Bitcoin. Mantener una postura clara entre él y otras altcoins requiere trabajo. Mantener la claridad, seguridad y pureza del único dinero verdaderamente sólido que el mundo ha conocido es fundamental si queremos tener una oportunidad en los tiempos que están por venir.

Adam Back - @adam3us
Allen Farrington - @allenf32
Anil - @anilsaidso
Arman the Parman - @parman_the
Bitcoin Gandalf - @BTCGandalf
Bitcoin Q+A - @BitcoinQ_A
BTC Sessions - @BTCsessions
BTC Times - @btc
Brandon Quittem - @Bquittem
D++ - @D_plus__plus
Dylan Le Clair - @DylanLeClair_
Gigi - @dergigi
Greg Foss - @FossGregfoss
Guy Swann - @TheGuySwann
Hugo Nguyen - @hugohanoi
Jameson Lopp - @lopp
Jeff Booth - @JeffBooth
Jimmy Song - @jimmysong
Knut Svanholm - @knutsvanholm
Luke Dash Jr - @LukeDashjr
Lyn Alden - @LynAldenContact
Marty Bent - @MartyBent
Matt Odell - @ODELL
Michael Saylor - @saylor
Natalie Brunell - @natbrunell
Nayib Bukele - @nayibbukele
Nic Carter - @nic_carter
Nick Szabo - @NickSzabo4
Nik Bhatia - @timevalueofbtc
Parker Lewis - @parkeralewis
Pleb Lab - @PlebLab
Preston Pysh - @PrestonPysh
Tomer Strolight - @TomerStrolight
Troy Cross - @thetrocro
Vijay Boyapati - @real_vijay
¡Gracias por enseñarme cada día!

PROYECTOS DE LA COMUNIDAD bitcoin:

A continuación se presentan algunos de los proyectos base en los que todo el mundo está trabajando para crear una economía circular y local con bitcoin.

Síguelos en Twitter para saber más o donar:

Bitcoin Beach El Zonte - El Salvador - @Bitcoinbeach

Bitcoin Ekasi - Mossel Bay, South Africa - @BitcoinEkasi Apoya a la ONG Surfer Kids)

Bitcoin Beach Brazil - Jericoacoara, Brazil -@BitcoinBeachBR

Bitcoin Jungle Costa Rica - Dominical, CR - @BitcoinJungleCR

Bitcoin Venezuela - Venezuela - @btcven

Bitcoin Smiles Dentistry - El Salvador - @BitcoinSmiles

Saul M - El Salvador - Chalatenango - @saulhodl

Apata Johnson - Nigeria - @ApataJ

Bitcoin Lake - Lake Atitlan - @LakeBitcoin

REFLEXIONES SOBRE bitcoin

Un saludo a
Satoshi y a
todos aquellos
soñadores de la
pastilla naranja,
videntes,
magos cypherpunk,
poetas por la libertad,
guardianes de la sabiduría,
individuos soberanos,
forjadores del último recurso,
solos, todos juntos, por la libertad.

Vires In Numeris!

REFLEXIONES SOBRE LA MADRIGUERA DE CONEJO

Bitcoin es realmente una "cosa" fascinante
Excepto que no es una "cosa"
En el sentido de que no puedes tocarla.
Sin embargo, está afectándonos a millones de nosotros
Alrededor del mundo
Y pronto, seremos billones…
Es cierto que
Son bits y bytes digitales
Algoritmos y código
Ceros y unos
Y que si cada uno de los nodos,
Minero, completado, ligero
Fueran, de alguna manera,
Destruidos,
Dejaría de existir
De la manera en que lo conocemos
Somos capaces de percibirlo…
Sin embargo, seguiría "existiendo"
En el sentido en el existen la física cuántica
O la gravedad
Independientemente de la percepción humana…
En el sentido de que las matemáticas ya existían
Antes de que los humanos las codificaran
Eligieron símbolos para representarlas
La verdad
Es que no nos necesita.

POR QUÉ TODO EL VALOR PASARÁ A BITCOIN

Hay algunas teorías de juego interesantes que parecen converger en lo que al bitcoin se refiere, haciendo que la probabilidad de su crecimiento y aumento de valor con el tiempo sea cada vez **más cierta.**

EL PUNTO FOCAL O PUNTO DE SCHELLING

Introducido en la década de 1960 por el economista estadounidense Thomas Schelling, el punto focal o de Schelling básicamente afirma que las personas que no necesariamente pueden comunicarse entre sí, pueden al menos converger en una decisión o curso de acción, especialmente cuando se presenta una solución convincente a un problema (-> bitcoin)

Además, al igual que este punto de Schelling llama la atención cada vez más, atrae a más gente (-> bitcoin)

EFECTO LINDY

En esencia, el efecto Lindy afirma que cuanto más tiempo lleva existiendo una idea, tecnología o negocio, es más probable que perdure.

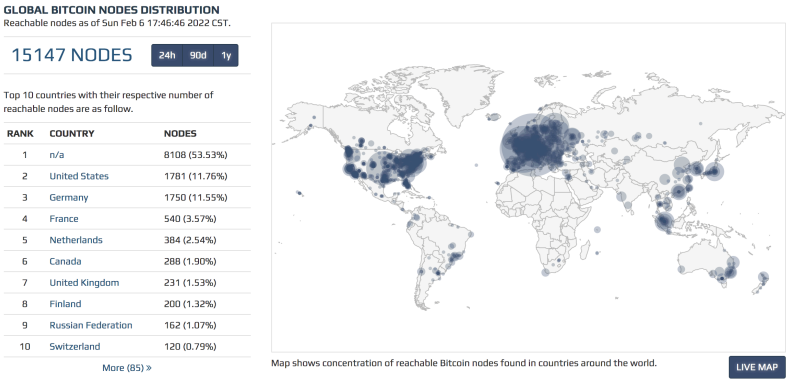
LEY DE METCALFE

Popularizada por Robert Metcalfe, inventor de Ethernet, entre otras cosas. La ley de Metcalfe afirma que una red es proporcionalmente más valiosa cuantos más usuarios tenga. La utilidad aumenta exponencialmente a medida que más y más usuarios se unen, fortaleciendo así la red.

LAS RED P2P [DE IGUAL A IGUAL]

Se trata de una base de datos global distribuida, con adiciones a la base de datos por consentimiento de la mayoría…

~ Satoshi Nakamoto, 18-2-2009



GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sun Feb 6 17:46:46 2022 CST.

15147 NODES | 24h | 90d | 1y

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	8108 (53.53%)
2	United States	1781 (11.76%)
3	Germany	1750 (11.55%)
4	France	540 (3.57%)
5	Netherlands	384 (2.54%)
6	Canada	288 (1.90%)
7	United Kingdom	231 (1.53%)
8	Finland	200 (1.32%)
9	Russian Federation	162 (1.07%)
10	Switzerland	120 (0.79%)

More (85) »

Distribución global de nodos Bitcoin accesibles

El resultado es un sistema distribuido sin un único punto de fallo. Los usuarios poseen las claves criptográficas de su propio dinero y realizan transacciones directamente entre ellos, con la ayuda de la red P2P para comprobar que no se produzcan dobles gastos.

~ Satoshi Nakamoto, 11-2-2009

BITCOIN, COMUNICACIÓN NO VIOLENTA Y PERMACULTURA

Considero que **Bitcoin,** creado para nosotros por Satoshi Nakamoto, es la base de una sociedad sana en lo que respecta a:

- **Comunicar valor**
- **Realizar transacciones e intercambios**
- **Almacenar nuestro tiempo** en un despliegue emergente, orgánico y honesto.

Considero que la **Comunicación No Violenta,** creada por el Doctor Marshall Rosenberg, es la base de una sociedad sana en lo que respecta a:

- **Comunicar sentimientos y necesidades**
- **Escucha profunda y empatía**
- **Encontrar soluciones co-creativas en un despliegue emergente, orgánico y honesto.**

Considero que la **Agricultura Natural y la Permacultura** que nos trajeron nuestros Ancestros y, más recientemente, Masunobu Fukuoka y Bill Mollison, son la capa fundacional de una sociedad sana en lo que respecta a:

- **Comunicar con la Tierra**
- **Cultivar alimentos, sanar la tierra**
- **Cuidar la naturaleza** en un despliegue emergente, orgánico y honesto.

Cada una de estas tecnologías, una matemática, que nos lleva más allá de las matemáticas, una lingüística, que nos lleva más allá del lenguaje, una biológica, que nos lleva más allá de la biología, se basan en la Verdad.

Depende de nosotros hacer uso de ellas, vivir en ellas y permitir que nos guíen cada vez más lejos hacia el potencial que sentimos como hormigas en las puntas de nuestra percepción.

Que encontremos el coraje, la fuerza,
la sabiduría y la gracia para avanzar
sin miedo en el viaje.

Manifiesto Cypherpunk

Por Eric Hughes

La privacidad es necesaria para una sociedad abierta en la era electrónica. La privacidad no es secretismo. Una cuestión privada es algo que no queremos que todo el mundo sepa, pero una cuestión secreta es algo que no queremos que nadie sepa. La privacidad es la capacidad de revelarse selectivamente al mundo.

Si dos personas están haciendo cualquier tipo de transacción, entonces tienen un recuerdo de su interacción. Cada uno de ellos puede hablar de su propio recuerdo sobre el tema. ¿Cómo podría prevenirse esto? Quizás se podrían presentar leyes en contra, **pero la libertad de expresión es aún más fundamental para una sociedad abierta que la privacidad;** nuestra intención no es restringir la libertad de expresión. Si muchas personas hablan juntas en un mismo fórum, cada una puede hablar a las demás y aumentar el conocimiento global acerca de esas personas. Las posibilidades de las comunicaciones electrónicas hacen posibles grupos así, y no van a desaparecer sólo porque nosotros queramos.

Ya que deseamos la privacidad, tenemos que asegurar a cada persona que intervenga en una transacción que sólo conozca lo que es estrictamente necesario para esa transacción. Ya que cualquier información puede expresarse, tenemos que asegurarnos de que revelamos lo mínimo posible. En muchos casos, la identidad personal no es significativa. Cuando compro una revista en un quiosco y pago al contado, el quiosquero no tiene ninguna necesidad de saber quién soy.

Cuando le pido a mi proveedor de correo electrónico la capacidad de recibir y enviar mensajes, mi proveedor no tiene por qué saber con quién hablo, qué digo o qué me dicen. Mi proveedor sólo tiene que saber dónde obtener el mensaje y cuánto le debo. Cuando mi identidad se revela debido al mecanismo de la transacción, no tengo privacidad. No puedo por tanto revelarme selectivamente ; estoy obligado a revelarme siempre.

Así pues, **la privacidad en una sociedad abierta requiere sistemas anónimos para efectuar transacciones. Hasta ahora, los billetes y las monedas han sido el mecanismo principal para asegurar la privacidad. Un sistema para transacciones anónimas no es un sistema para transacciones secretas. Un sistema anónimo ofrece la capacidad a los individuos para revelar su identidad sólo cuando lo deseen ; esta es la esencia de la privacidad.**

Así mismo la privacidad en una sociedad abierta requiere la criptografía. Si yo digo algo, quiero que lo oigan sólo aquellos a los que iba dirigido lo que decía. Si el contenido de mi discurso está al alcance de todo el mundo, no tengo privacidad. Encriptar es indicar que se desea la privacidad y encriptar con sistemas criptográficos « débiles » es indicar que no se tiene un gran interés en la privacidad. Además, **revelar la propia identidad de forma que no hayan dudas cuando lo estándar es el anonimato requiere del sistema de firmas criptográficas.** No podemos esperar que los gobiernos, la corporaciones y otras grandes organizaciones sin cara nos garanticen la privacidad sin sacar beneficios de ello.

A ellos les resulta beneficioso hablar de nosotros, y podemos esperar que lo harán. Intentar evitar sus discursos es luchar contra la esencia de la información. La información no sólo quiere ser libre, anhela ser libre. La información se expande hasta ocupar todo el espacio disponible. La información es el primo más joven y más fuerte del Rumor. La información tiene más ojos, sabe más y entiende menos que el Rumor.

Tenemos que defender nuestra privacidad si es que queremos tenerla. Tenemos que unirnos y crear sistemas que permitan las transacciones anónimas. La gente ha estado defendiendo su privacidad durante siglos mediante susurros, oscuridad, sobres, puertas cerradas, apretones de manos en clave y mensajeros. Las tecnologías del pasado no permitían una encriptación « fuerte », pero las actuales sí.

Nosotros los cypherpunks nos dedicamos a construir sistemas anónimos. Defendemos nuestra privacidad con criptografía, con sistemas de envío anónimo de e-mail, con firmas electrónicas y con dinero electrónico.

Los cypherpunks programan. Sabemos que alguien tiene que escribir software para defender la privacidad, y puesto que no podemos obtener privacidad hasta que todos la tengamos, vamos a programar. Publicamos nuestro código de manera que nuestros compañeros cypherpunks puedan practicar y jugar con él.

Nuestro código es gratis para que todo el mundo pueda usarlo. No nos importa si no apruebas el software que escribimos. Sabemos que el software no puede ser destruido y que un sistema ampliamente disperso no puede cerrarse.

Los cypherpunks deploran las regulaciones en criptografía, pues la criptografía es fundamentalmente un acto privado. El acto de encriptar de hecho retira la información del dominio público. Incluso las leyes contra la criptografía no pueden ir más allá de las fronteras nacionales y de su brazo armado.

La criptografía va a extenderse en todo el mundo, y con ella los sistemas de transacciones anónimas que la hacen posible.

Para que la privacidad se extienda tiene que formar parte de un contrato social. La gente tiene que unirse y usar estos sistemas para el bien común. La privacidad sólo se extenderá mientras los miembros de la sociedad cooperen entre sí. Nosotros los cypherpunks esperamos vuestras preguntas y vuestras preocupaciones y esperamos engancharte para que no nos autoengañemos. Sin embargo no pensamos apartarnos de nuestro curso porque algunos no estén de acuerdo con nuestras metas.

Los cypherpunks están activamente enganchados en el logro de unas redes más seguras para la privacidad. Trabajemos juntos.

Onward.
Eric Hughes <hughes@soda.berkeley.edu>
9 Marzo 1993

(Lo subrayado en **negrita** es cosa mía)
Traducción original al español por JS en: https://medium.com/@rootsec/un-manifiesto-cypherpunk-por-eric-hughes-3aa4660af977

ALGUNOS DE LOS PRIMEROS CYPHERPUNKS

A los que podemos dar las gracias por contribuir al desarrollo del efectivo digital P2P [de igual a igual]

- **Satoshi Nakamoto** - Cypherpunk anónimo que introdujo Bitcoin al mundo en 2009.
- **Nick Szabo** - Bit Gold 2005
- **Hal Finney** - 2004 Reusable Proof of Work (RPoW), Author of PGP 2.0. Segunda persona en ejecutar Bitcoin. Recibió la primera transacción de 10 bitcoins de Satoshi Nakamoto.
- **Wei Dai** - B-money 1998
- **Dr Adam Back** - HashCash 1997 - CEO Blockstream
- **Douglas Jackson and Barry Downey** - E Gold 1996
- **John Gilmore**
- **Timothy C.May**
- **Eric Hughes**

  } Fundadores del movimiento Cypherpunk y la lista de correo en 1992.

- **Philip Zimmermann:** 1991 PGP 1.0, tel cifrado de correo electrónico más utilizado en la actualidad.
- **David Chaum** - Ecash 1983 y DigiCash 1989

El White Paper de bitcoin

Presentado al mundo a través de metzdowd.com
31-10-2018

Por Satoshi Nakamoto

Un Cypherpunk anónimo, que se comunicó con la comunidad cypherpunk por última vez en el foro bitcointalk.org el 10-12-2010.

Al marcharse, permitió que Bitcoin fuera un verdadero experimento en lo salvaje. Todos los que trabajan en él son voluntarios en algún sentido, <-> inspirados por el potencial de liberar a la humanidad de los grilletes de un sistema monetario manipulado, basado en la deuda, y en su lugar, participar en una red global, sin confianza, sin permisos, resistente a la censura, verdaderamente escasa, entre pares, descentralizada de dinero y pagos monetarios, que está inspirando a un orden emergente a resurgir de las cenizas fiat.

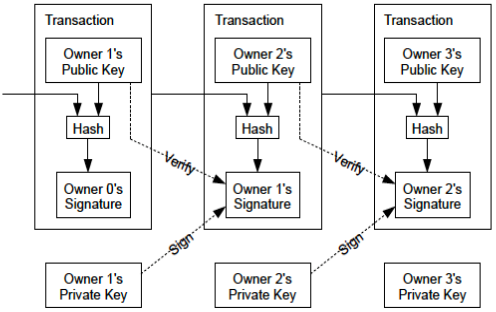
TODOS SOMOS SATOSHI

`The Times, 3-1-2009, El Canciller, al borde del segundo rescate bancario.`

~ Texto de un titular de The Times of London, grabado en el bloque Génesis de Bitcoin por Satoshi Nakamoto el 3-1-2009

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

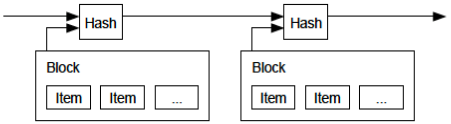


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

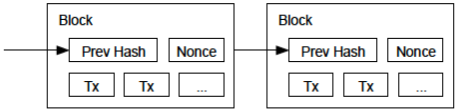
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

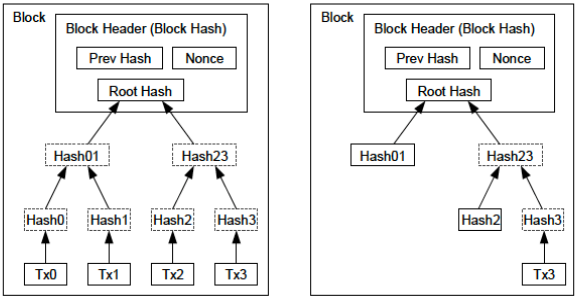
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



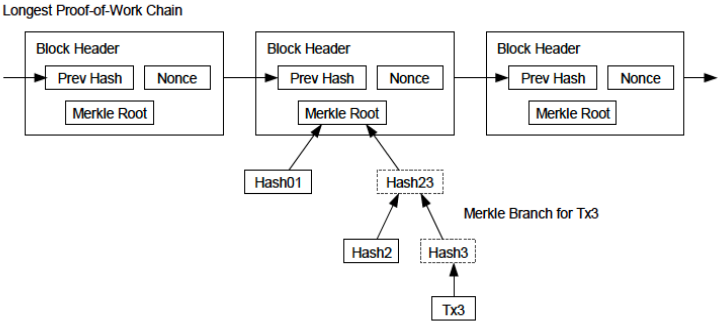
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

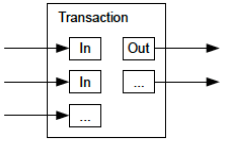
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

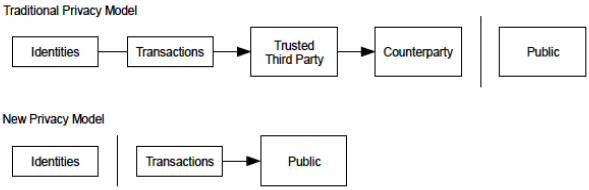
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

BLOQUE GÉNESIS DE BITCOIN, PRIMERA VERSIÓN, 3-1-2009

```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00            ŠLp+kñ._¬....
```

Y así se dio
comienzo,

a una nueva era…

Mi más profundo agradecimiento a Satoshi, a los pasados y futuros cypherpunks, al vórtice BT, a los tóxicos, no tóxicos, los señores y señoras de los memes, los creyentes, los cínicos, los videntes…

Y siempre, a mi querida familia, amigos, y Aquel que respira a través de todos nosotros, por verme siempre salir adelante, más valioso que cualquier cosa, incluso bitcoin.

Consulta el libro de bolsillo en:
thesimplestbitcoinbook.net
Siéntete libre de enviar comentarios, preguntas, actualizaciones, sugerencias a:
TheSimplestBitcoinBook@proton.me
No puedo prometer que te responda o me ponga con ello a tiempo…
quizá esté por ahí yendo descalzo en alguna montaña.

Guarda tus sats
Aguanta
Y quédate con la verdad

Y por último, mucho amor.

Bloque # 728922

hola!

Si leer esto fue importante para ti y te gustaría comprar el libro en formato físico

o donar algunos sats para apoyarme a medida que creo nuevo contenido,

por favor, visita mi página web escaneando el código QR a continuación.

¡Gracias!