

# GUÍA BITCOIN

JORGE CANER

Todo el mundo bitcoin

# TODO LO QUÉ NECESITAS SABER SOBRE BITCOIN Y CRIPTOMONEDA

¿Has oído hablar de Bitcoin pero no sabes muy bien “qué es uno de esos”? Si es así, estás en el sitio adecuado..!

Bitcoin es el MEJOR y MÁS JUSTO dinero que existe. ¿Te parece atrevida la frase? Te reto a que le dediques un par

de tardes a estudiarlo y rebatas la frase si aún sigues pensando que es atrevida.

Con la elaboración de ésta guía no pretendo que al final de su lectura termines siendo un experto en Bitcoin y Criptomonedas, sólo busco de una manera básica que adquieras los conocimientos necesarios que te permitan entender que estás ante uno de los fenómenos **MÁS IMPORTANTES** a nivel global y **HOY** tú también puedes ser parte de ello.

Esta guía es sólo un abre boca de todo lo que vas a poder aprender más adelante y cómo vas a ser capaz de **EMPEZAR A GANAR** gracias al **BitCoin** y las **Criptomonedas** con el

MENOR DE LOS RIESGOS posible.

A lo largo de ésta guía aprenderás qué es Bitcoin, cuáles son sus ventajas, cómo se usa, cómo se almacena de forma segura, cómo funciona internamente, quién lo ha creado y mejora constantemente, cómo se analiza la transparencia de Blockchain,... y un largo etcétera de información.

Como introducción decirte que los Bitcoins son, en esencia, dinero digital. Dinero utilizado para realizar pagos de forma barata y muy rápida a través de todo el planeta sin necesidad de bancos o tarjetas de crédito. Estas monedas las gestiona un software llamado de la

misma forma, Bitcoin.

Bitcoin separa por completo dinero y política, y es mundial. Esto hace que, por primera vez en la historia, pueda ser usado de verdad un dinero sencillo de utilizar y que de libertad absoluta a la gente al no depender de una moneda gestionada por políticas económicas decididas por organizaciones privadas o bancos centrales.

Bitcoin está poniendo patas arriba el sistema financiero mundial.

Conocida como la moneda de Internet, nace en 2009 de la mano de Satoshi Nakamoto siendo un sistema completamente descentralizado y digital.

Sus claras ventajas como dinero y tecnología ha generado que, en apenas 8 años, millones de personas y compañías ya lo utilicen cada día, dando como resultado la revalorización de sus monedas en un 10,000%: un solo BitCoin ha pasado de valer \$0 (Enero de 2009) a valer \$20000 (Diciembre de 2017).

Internamente, Bitcoin, administra una base de datos, la conocida Blockchain. Esta base de datos es un libro de contabilidad que se replica por cada instalación del software, lo que ha permitido contar ya con miles de instalaciones por todo el mundo que son capaces de mantenerse sincronizadas al

instante.

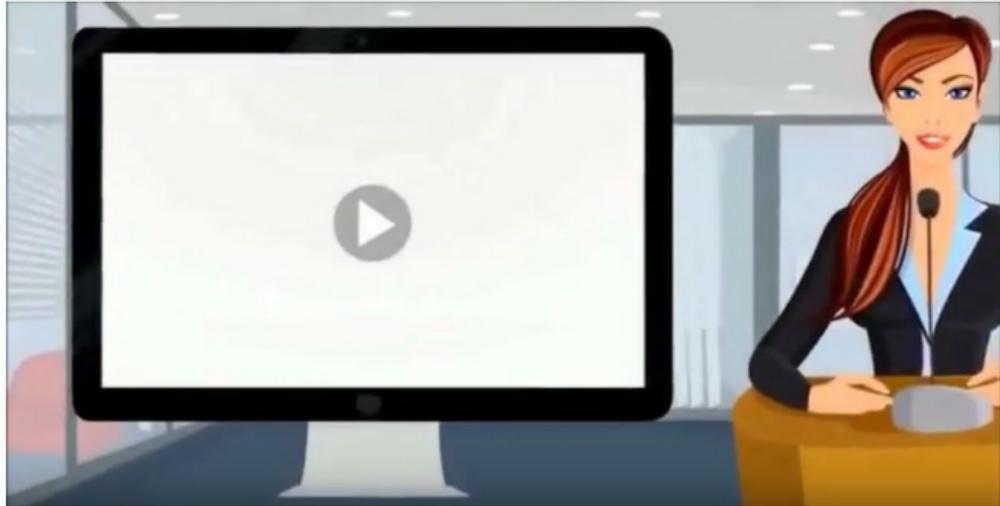
Prepárate para adentrarte en lo que posiblemente es la mayor revolución tecnológica, social y política que ha ocurrido desde la invención de Internet. Desconecta cualquier cosa que pueda molestarte y presta atención por que esto va a cambiar tu vida.

# ¿Qué es BitCoin?

Bitcoin, en esencia, es dinero, es un nuevo tipo de dinero digital. Un dinero digital que permite realizar pagos de forma segura, barata, rápida y libre alrededor de todo el planeta.

Para ponernos en situación vamos a ver el siguiente vídeo:

**Haz clic sobre la  
imagen para  
visualizarlo**



Bitcoin es a la vez un protocolo, una red de pagos y una moneda. Originalmente se propuso como concepto en 2008, pero fue lanzada en Enero de 2009 por Satoshi Nakamoto

A finales de 2016 contaba con más de 10 millones de usuarios y más de 100.000 comercios de todo el mundo lo aceptan como medio de pago.

Actualmente, cada mes, llegan más de un millón de nuevos usuarios a Bitcoin.

La red Bitcoin es la red más segura del mundo, y a finales de 2016 ya procesaba más de 300.000 transacciones diarias.

Su diseño es tan revolucionario que, en solo unos pocos años, está poniendo patas arriba el sistema financiero que todos conocemos, desplazando completamente a los bancos, tarjetas de crédito, SEPA, SWIFT e incluso a figuras como los bancos centrales.

Es libre, es abierto pero sobretodo es descentralizado y cuida tu privacidad. No está controlada por ningún banco, gobierno ni empresa. Depende de una red formada por ordenadores de

personas. Una red descentralizada y gestionada por sus usuarios. O dicho de otra forma: no existe un banco central que emita el dinero alegremente.

Lo que hace especial a Bitcoin no es que sea una divisa digital. El euro, dólar o otras monedas también son, en gran parte digitales, y es un dinero digital que existe desde hace décadas. Casi todo el dinero que existe es digital. Tampoco lo hace especial que tenga costes reducidos de transacción, o que realice transacciones rápidas.

Estas y otras características, eventualmente, también acabarán ofreciéndolas los bancos. La principal

diferencia, lo que de verdad hace mágico a Bitcoin, es que es una red P2P: nadie emite el dinero. Separa política y dinero. Y esto, al entender cómo funciona el dinero y los bancos centrales, te hace entender como Bitcoin hace libre a la humanidad.

Jamás existirán más de 21 millones y se irán creando durante los siguientes 100 años; cada BitCoin es divisible en 100 millones de unidades; su cotización fluctúa por la oferta y la demanda.

### **Algunas conceptos claves:**

**Bitcoin.** Se refiere a la red de transacciones; puede ser usada para aplicaciones de todo tipo; en las

transacciones se envían Bitcoins; todas las transacciones son guardadas pseudónimamente en un libro de cuentas llamado Blockchain.

**Blockchain.** Libro de cuentas público y distribuido donde todas las transacciones BitCoin (y sus saldos) son almacenados de forma permanente. gracias a la “minería”. Blockchain es conocida como la base de datos más segura y veraz que existe.

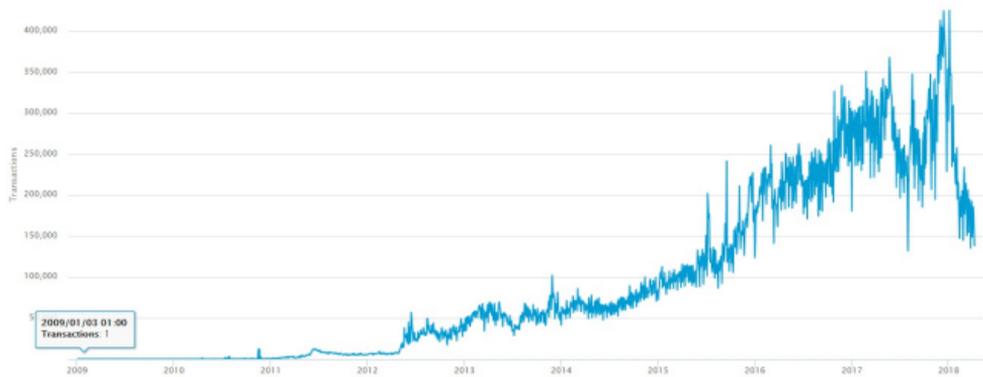
**Minería.** Proceso por el cual las transacciones de la red Bitcoin son verificadas; para ello se utilizan técnicas avanzadas de criptografía y hardware especializado (mineros): una cantidad fija de Bitcoins son creados

(minados) durante el proceso

# Por qué Bitcoin le gusta a la gente

Ya sabemos que cada vez se habla más de Bitcoin, ¿por qué a la gente le gusta tanto Bitcoin?

**Gráfico con el número de transacciones desde los inicios del BitCoin**



## Vamos a conocer 13 claves del BitCoin para entender esto

### 1. Rápido

Enviar cualquier cantidad de dinero es cuestión de minutos. Sin importar la cantidad, sin importar el destino.

### 2. Barato

El coste de realizar una transferencia a cualquier parte del mundo a través de tu banco puede costarte mucho dinero. Al hacerlo en Bitcoin el coste es de céntimos o gratis. Micro pagos: usando

un banco, pagar 0.3 € a alguien de Chile en agradecimiento por un tuit o like es IMPENSABLE, en Bitcoin es realidad.

### **3. Global**

Puedes enviar Bitcoins a cualquier país del mundo. Bitcoin, como Internet o el email no tiene fronteras. Esto con la garantía de respetar la libertad de sus usuarios, hace de Bitcoin la primera moneda global que funciona de verdad.

### **4. Emisión descentralizada**

Ningún gobierno ni banco central puede controlarlo o interferir en la valoración del BitCoin, ni en su creación ni en su distribución. Con Bitcoin se despolitiza

el dinero, se hace de la gente, eliminando de esta forma el control que con el dinero FIAT se ejerce sobre la población.

## **5. Tuyo**

Tus Bitcoins son sólo tuyos. El dinero te pertenece al 100%; no puede ser intervenido por nadie, no hay corralitos ni las cuentas pueden ser congeladas. En Bitcoin tu puedes ser tu propio banco.

## **6. Dinero programable**

Bitcoin es sencillo de implementar y lleva implícito todo un lenguaje de programación, lo que permite crear pedazos de código que se ejecutarán en

la transacción. Esto antes era impensable, permite a cualquier programador monetizar todo tipo de servicios. Incluso pagos entre máquinas totalmente autónomas es posible, simplificando procesos manuales, complejos y lentos.

## **7. Cifrado y distribuido**

Bitcoin es muy seguro. Tiene en su núcleo, y en cada una de las operaciones uno de los sistemas criptográficos más potentes que existe, más que el usado por bancos o servicios cruciales de nuestro día a día. Su carácter distribuido lo hace resistente a caídas de la red o a ataques: JAMÁS ningún otro sistema

informático ha estado operativo las 24 horas del día, los 365 días del año durante más de 8 años.

Incluso ante una tormenta solar Bitcoin al contrario de otros sistemas, resistiría. Esto es debido a que algunos de sus nodos se encuentran en bunkers de la segunda guerra mundial, protegidos bajo tierra e incluso triple seguridad perimetral.

## **8. Transparente**

Todas las transacciones son públicas, ya que son visibles en tiempo real bajo pseudónimos en forma de dirección Bitcoin. Cualquiera puede desvelar la dirección Bitcoin que gestiona

mostrando con absoluta transparencia donde va hasta el último céntimo. Imagina gobiernos, ayuntamientos, ONGs, fundaciones, asociaciones, empresas,... cualquiera puede aprovechar esta funcionalidad en segundos.

## **9. Código abierto**

Bitcoin es un software totalmente abierto, libre y gratuito. Cualquiera puede ver su código fuente, estudiarlo, auditarlo o mejorarlo. Cientos de personas lo mejoran a diario: algunos de los cerebros más inteligentes del planeta lo hacen mejor a diario bajo un entorno de consenso democrático.

## **10. Basado en consenso**

Desde el desarrollo del código hasta la forma que tiene su Blockchain opera el consenso como eje fundamental. En su desarrollo, las ideas y mejoras del códigos más votadas por el resto son las que terminan implementándose: Bitcoin cambia si la mayoría acepta este cambio. Lo mismo ocurre con el libro de contabilidad que gestiona, el Blockchain: solo si la mayoría de nodos dan por válida una nueva transacción ésta queda aceptada y registrada en el libro de cuentas.

## **11. Emisión limitada**

En Bitcoin nadie puede generar miles de

Bitcoins una mañana porque de repente le apetezca a un político o a un banquero. Jamás existirán más de 21 millones y todos van apareciendo por la minería, siempre bajo unas reglas que son totalmente públicas.

## **12. Sin barreras**

En Bitcoin tu eres tu propio banco. Pero al hacerlo no pagas por un coste de apertura de cuenta, comisiones mensuales de mantenimiento o gastos falsos como si ocurre en un banco. No pagas por tener tarjetas de crédito (de hecho no se necesita, es una tecnología obsoleta)... Tener un monedero es gratis y con ello puedes almacenar todos los

Bitcoin que te apetezca, así como mandar Bitcoin a cualquier parte del planeta sin que nadie te lo impida.

Nadie te va a cobrar una suscripción, ni contratos, ni permanencias, ni retenciones, ni tus datos a cambio de una cubertería

### **13. Privado**

En tiempos de robos de información constante, espionaje industrial y a la sociedad por parte de los gobiernos y delincuentes informáticos y, aun más, con la aparición de técnicas avanzadas de Big Data, es más importante que nunca cuidar nuestra privacidad, llegando a mantenerla en un grado muy

alto.

Bitcoin tiene este concepto muy interiorizado. Bitcoin no es completamente anónimo, pero trabaja para serlo.

# ¿Qué es la Cadena de Bloques (Blockchain)?

Este es el principio fundamental que respalda la Cadena de bloques o Blockchain, una tecnología que tiene el poder de cambiar para siempre nuestra relación con el mundo digital.

Imagina un fichero de texto con dos columnas, donde en una columna pone un identificador (ejemplo “abc”) y en la otra un número (ejemplo “34”). Es decir “abc” le corresponden “34”. Ahora

imagina que ese fichero pudiera estar en miles de ordenadores duplicado, con la seguridad de que nadie lo puede alterar a traición pero cuando legítimamente se debe alterar algo, en cuestión de segundos, todos se sincronizan. Aunque uno de los miles de ordenadores desapareciese de la red no pasaría nada. Esto es lo que consigue Blockchain y aunque su magia es mucho más compleja y compuesta de más piezas como la criptografía, en esencia eso busca: un registro distribuido resistente a la sincronización y sin necesidad de confianza entre los miembros que la conforman. Algo que llevaba décadas intentándose resolver y en Bitcoin lo ha conseguido su creador, el desconocido

Satoshi Nakamoto

**Que es Blockchain? - Video de la BBC  
con Doblaje Español Haz clic sobre la  
imagen para visualizarlo**



# ¿Cómo Comprar y Vender Bitcoins?, ¿Cuánto vale un Bitcoin?, ¿Cómo y quién determina su precio?

Si hubieses comprado 100€ de Bitcoins en enero de 2010 y vendido en noviembre de 2013, hubieses tenido 120.000.000 €.

No está nada mal ¿verdad? De 100€ a

120 millones de euros...  
multimillonario en 3 años con una  
inversión de risa.

¿Como se determina el precio de Bitcoin para que se den situaciones así? No solo ocurrió y tiene su explicación, sino que muchos piensan que una nueva situación similar está por llegar.

Como ya hemos explicado, Bitcoin es un sistema financiero distribuido, liberado en 2009 por un programador bajo el pseudónimo de Satoshi Nakamoto. No está emitido por ningún gobierno ni empresa (pese a que cada vez está más respaldado por estos) y no es considerado moneda de curso legal en ningún país hasta la fecha (aunque ya

empieza a encajarse en marcos legales existentes, como la reciente sentencia que determina al Bitcoin exento de IVA en toda Europa).

Bitcoin es poderoso y una pieza maestra de la ingeniería, pero ¿Cuánto vale un BitCoin?, ¿Por qué sube y baja su precio tantas veces al día?, ¿Quién determina su precio?, ¿Qué seguridad tiene ese precio? ¿Es una estafa, ponzi o mecanismo extraño para robarme el dinero? (Que de todo se ha escuchado)

Vayamos por partes.

# Bitcoin como dinero

Pero... ¡un momento! si un dinero no te lo aceptan como medio de pago, por mucho que sea genial como unidad de cuenta, y todo lo que quieras... ¿vale algo?. Es por ello que el valor del dinero no es que vaya muy ligado a su aceptación, sino que está directamente relacionado.

El dinero FIAT (que es el dinero oficial como los euros o dólares entre otros), tal como lo conocemos hoy, no son más billetes y monedas sin valor propio, ya

muy lejos de cuando representaban un valor en oro. Están avalados y certificados únicamente por entidades emisoras.

No importa la franja temporal de la historia que selecciones, este modelo ha demostrado fallar estrepitosamente. Solo en el siglo XXI (y fíjate que solo llevamos 16 años de siglo) ya van múltiples fracasos: Crisis, corralitos, inflaciones descontroladas,...

Población sometida. Las divisas emitidas por los bancos centrales son necesarias para que estos puedan aplicar, de forma opaca, políticas económicas concretas, dejando al antojo de unos pocos el destino de millones de

personas. A golpe, literalmente, de click pueden generar nuevos millones de euros en un ordenador que devalúen el poder adquisitivo de las personas.

Paradójicamente, la mayoría vemos al dinero actual (euros, dólares,...) como una solución cuando, en la realidad, es algo parecido a un yugo que nos somete a los deseos de unos pocos al tiempo que nos hacen partícipes de guerras y barbaries desmedidas una y otra vez.

# Oferta y demanda. Pero, ¿Quién determina su precio?

El precio de un BitCoin lo determina todo aquel que quiera participar en su proceso de compra y venta, en esencia sus usuarios. Esto es, lo que en última instancia, determina siempre el precio del BitCoin, aunque para ello múltiples factores influyan.

El comercio de Bitcoins permite

distribuirlo y beneficiarse por ello. Como en otros escenarios, los productores (en el caso de Bitcoin: los mineros) pueden proponer un precio al vender sus Bitcoins a los interesados llegando a acuerdos.

Imagina los típicos tratos entre dos personas, una propone un precio y si la otra, entre regateos, está dispuesto a aceptarlo entonces se hace la transacción.

Esto puede hacerse en la calle, y se hace. Pero, en un mundo informatizado como el nuestro, es más común ver este tipo de tratos en plataformas online especializadas y optimizadas para ello. Las conocidas “plataformas de trading

Bitcoin”. Hay decenas: [Binance](#), Kraken o Poloniex son algunas de ellas.

A diferencia de una web de compra – venta, que tiene sus precios estipulados como en [Coinbase](#), en una plataforma de trading cualquiera puede publicar una propuesta de compra al precio deseado.

En los mercados de trading tampoco tienes obligación de comprar un BitCoin completo, puedes comprar pedazos. Recuerda que 1 BitCoin está compuesto de 100 millones de “céntimos” (satoshis). Si un Bitcoin vale 1000€, puedes comprar 1 euro si lo deseas.

Cuando otra oferta de venta coincida con la tuya, automáticamente, se hace la

transacción. Esta operación de compra – venta se hace solo en esa plataforma que el precio del Bitcoin se fije al precio del intercambio realizado.

Esto que acabamos de describir es el mismo proceso en el que se comercia todas las materias que existen. Y ocurre decenas, centenares o millares de veces por al día, a veces con grandes variaciones.

Este tipo de operaciones requieren de un mínimo de estudio y tareas previas, que aunque sin coste, no todos los usuarios están dispuestos a hacer. Para muchos usuarios esta parte de Bitcoin no es atractiva e incluso les repele, puesto que parece que no aporta nada y la mayoría

de las veces es simple especulación. Comprar barato y vender caro. Pero lo cierto es que este modelo está haciendo que Bitcoin se difunda y llegue a más sitios.

El valor del BitCoin ha ido cambiando a lo largo del tiempo y se basa, a grosso modo, en la confianza de sus usuarios, en su utilidad y su popularidad.

Significa que, en 2010, el valor de un BitCoin era menos de un céntimo de euro, pues muchos aún dudaban de su seguridad, eficiencia y, en definitiva, su aceptación.

Esta operativa de determinar el precio a través de la compra – venta no es

diferente a la que ocurre en otros sectores: divisas de curso legal (Forex), materias primas, bonos,... Pero en Bitcoin tiene un doble objetivo, puesto que esto al mismo tiempo, al tratarse de algo digital, ha sido clave para su capitalización, llegando los Bitcoins a más personas.

Hay mucho recorrido. ¿Qué pasaría con el precio de Bitcoin si mañana Amazon decide aceptarlo como medio de pago? Nadie sabe que pasará, ni tan si quiera si ocurrirá, pero es posible que ocurra igual que con miles de grandes empresas, países,...

Aunque ya es posible comprar en Amazon pero a través de terceros como

es el caso **Purse**

# Bitcoin como medio de pago

El primer precio de un BitCoin de la historia fue determinado por una transacción entre particulares. Ocurrió el 22 de Mayo del 2010, en el foro BitcoinTalk, donde el usuario jercos decidió comprarle con su tarjeta de crédito dos pizzas al usuario laszlo a cambio de 10,000 Bitcoins, posiblemente con una tasa de cambio de  $1\text{BTC} = \$0.003$ .

Este simple hecho supuso la chispa que encendió un proceso acelerado de

revalorización. Los entonces poseedores de Bitcoins se dieron cuenta de que podrían acceder a bienes o servicios con sus actuales criptodivisas, hasta la fecha sin valor económico, dejando patente que Bitcoin definitivamente sí tenía capacidad de convertirse en lo que su ideólogo y creador, Satoshi Nakamoto, había propuesto: un sistema financiero mundial alternativo y mejorado.

Esto hizo que mucha gente vendiese Bitcoins que antes no tenían valor por unos pocos euros. ¡Imagínate! Tienes 10.000 Bitcoins que has obtenido gratuitamente o a un euro, y de repente puedes obtener por todos 100€. Tú, sin

ser adivino, ¿que harías?

Solo algunos visionarios (o, seguramente, despistados en su mayoría) pudieron encontrarse situaciones como las de 2013, con millones de euros entre las manos o intentando encontrar un ordenador con miles de Bitcoins que hubiesen tirado a la basura por error. Pese a eso, 2013 fue un año de muchos nuevos millonarios gracias a Bitcoin.

# Historial del precio de Bitcoin

A tan solo 9 años de su creación, Bitcoin se caracteriza también por su alta volatilidad. A lo largo de su corta, pero intensa existencia, un solo BitCoin ha pasado de valer literalmente nada a casi 1200 dólares americanos.

Algunos teóricos asocian esto a su fase temprana y que es algo característico de los nuevos modelos económicos, necesitando de unos años para empezar a estabilizarse.

**Enero, 2009 – Enero, 2010. Nada (0€)**

No existían casas de cambio.

Únicamente los fans se lo intercambiaban en foros a modo de prueba.

**Febrero, 2010 – Mayo, 2010. Menos de \$0.003**

El 22 de Mayo del 2010, el usuario “laszlo” hizo la primera transacción por un bien, comprando dos pizzas en Jacksonville, Florida por 10,000 BTC. El usuario “SmokeTooMuch” intentó subastar 10,000 BTC por \$50, pero nadie los compró.

**Julio, 2010. \$0.08**

En cinco días el precio del BitCoin

creció un 1000% pasando de \$0.008 a \$0.08 por un Bitcoin.

**Febrero, 2011 – Abril 2011. \$1**

Bitcoin logra algo que se creía imposible, la paridad con el dólar.

**8 Julio, 2011. \$31**

Máximo de la primera “burbuja”, seguido de su primera caída de precio.

**Diciembre, 2011. \$2**

El mínimo tras unos meses. Se propaga una desconfianza en Bitcoin.

**Diciembre 2012. \$13**

Crece lentamente durante un año.

**Abril, 2013. \$266**

Máximo de un ascenso vertiginoso donde el precio aumenta entre un 5% y

10% cada día.

**Mayo, 2013. \$130**

Unos meses de estabilidad.

**Junio, 2013. \$100**

En Junio cae hasta \$70 pero en Julio aumenta hasta \$110.

**Noviembre, 2013. \$350 – \$1250**

Este mes fue el que llevó a Bitcoin a su máximo hasta la fecha. Desde Octubre hasta Noviembre pasó de \$150 a \$200, creciendo en este mes hasta \$400, luego \$600, \$900 y finalmente rompiendo el techo de los \$1000 el 27 de Noviembre del 2013.

**Diciembre, 2013. \$600 – \$1000**

El precio cae en picado a \$600, rebota hasta los \$1000 y cae de nuevo hasta \$500. Se queda oscilando entre \$650 y \$800.

### **Enero, 2014. \$750 – \$1000**

El precio rozó los \$1000 a principios de enero brevemente para posteriormente situarse entre los \$800 y \$900 durante el resto del mes.

### **Febrero, 2014. \$550 – \$750**

Tras el cierre de MT. Gox el precio se ve afectado y se sitúa entre \$600 y \$700.

### **Marzo, 2014. \$450 – \$700**

El precio cae debido a un falso reporte donde el gobierno chino censuraba Bitcoin, donde obligaban a los bancos a

cerrar las cuentas de todas las casas de cambio que trabajasen con Bitcoin.

**Abril, 2014. \$340 – \$530**

El precio más bajo desde 2012-2013 fue alcanzado el 11 de Abril a las 3:25AM.

**Mayo, 2014. \$440 – \$630**

En los últimos días de mayo el precio del Bitcoin crece un 30%.

**Marzo, 2015. \$200 – \$300**

El precio vuelve a caer a principios del 2015.

**Noviembre, 2015. \$395 – \$504**

Durante 2015 el precio fue aumentando de forma regular llegando a los \$504 en Noviembre.

## **Febrero 2017. \$1222**

Durante 2016 y principio de 2017, el precio dio grandes subidas llegando a multiplicarse por 3 debido a los sucesos políticos mundiales: Brexit, Trump como presidente de Estados Unidos, China y sus crisis, India y sus políticas económicas, crisis de nuevos bancos,... Además del halving de Bitcoin en Julio de 2016.

## **Marzo 2017. \$1270**

Con la llegada del ETF promovido ante la SEC por los hermanos Winklevoss, Bitcoin bate todo tipo de récords: Mayor precio de la historia superando incluso al oro, mayor capitalización de la historia, mayor número de usuarios,

mayor número de respaldo y aceptación.

**Diciembre 2017.**

**\$20,000**

# Futuro del precio del Bitcoin

No es una tarea sencilla. De poco sirve analizar el precio actual y el histórico si no es para observar una tendencia a lo largo de su historia.

Pese a que Bitcoin usa tecnología superior a la que usan gobiernos y bancos, nadie sabe qué puede pasar en el futuro. No sabemos cómo evolucionará la tecnología, el consumo energético,...

Algunas estimaciones indican que 3 de

cada 4 Bitcoins se están usando como ahorro, como reserva de valor, por lo que es posible que mucho menos de 6 millones de Bitcoins (21 millones / 4) se queden disponibles para transacciones durante mucho tiempo.

Mientras algunos prevén un fracaso de Bitcoin, otros justamente lo contrario. Entre ellos Rickard Falkvinge, líder y fundador del Partido Pirata, que sostiene que entre 2020 y 2025 podría estar su precio entre 100.000 y 1.000.000 de euros o escenarios más optimistas que lo colocan en un valor de 47 Millones de euros por cada Bitcoin en la siguientes décadas.

Además prevén una estabilidad de su

precio tras la etapa de crecimiento.

Los detractores de Bitcoin defienden que es algo que podría desaparecer en cualquier momento. ¿Pero como haces desaparecer por arte de magia algo que tienen millones de personas y cada mes llegan nuevos usuarios de forma exponencial? Un sistema abierto, transparente, con algunas de las mejores mentes del planeta trabajando en el, muchos por placer, ¿Como paras eso? Bitcoin, cuando se analiza con tiempo ves que parece ser mucho más fuerte, justo y poderoso para el usuario incluso que el dinero fiduciario de un país.

Recordemos que un BitCoin es

divisible, y tiene 100 millones de satoshis (su unidad más pequeña), pudiendo llegar un futuro donde equipararse 1 Satoshi con 1 céntimo de euro y valer el millón de euros que anteriormente mencionamos, ¡pero ojo! Bitcoin funciona por consenso, y esa cantidad de decimales podría aumentarse si llegase a ser necesario y la mayoría de los nodos estuviese de acuerdo.

Actualmente centenares de tiendas aceptan Bitcoin como medio de pago.

¿Crees que, un sistema capaz de gestionar la contabilidad económica mundial de forma más óptima, transparente, descentralizada y barata

que la tradicional, y que gana millones de usuarios cada año, desaparecerá? Y si no desaparece, ¿hasta donde crees que llegará el precio de un solo BitCoin?

# ¿Cómo comprar Bitcoins?

¿Cuánta gente conoces que sepa comprar Bitcoins?

A mí me pasa lo mismo.

En cuanto te sales del circuito de personas que conocen Bitcoin en profundidad es difícil dar con alguien que sepa cómo hacerlo.

Suelo utilizar [Coinbase](#) sobretodo porque es una de las más importantes y está regulada.

También suelo utilizar [Uphold](#), es otra plataforma en la que confío mucho. Son

plataformas que además de estar reguladas, y poder comprar, también se pueden utilizar para almacenar criptomonedas (wallets)

# Tutoriales Coinbase

<http://www.losgladiadoresdelinternet.com>

# Tutoriales Uphold

<http://www.losgladiadoresdelinternet.com>

**Compra tus Bitcoins  
ahora haciendo click  
aquí.**

## **Cómo proteger tus bitcoins**

Tras revisar las diferentes formas de comprar bitcoins, es la hora de hablar sobre las recomendaciones más importantes para mantenerlos seguros

Bitcoin es una de las monedas que más difícil se lo han puesto a los ladrones

desde que el dinero fue creado, pero al igual que cualquier sistema, su seguridad puede ser reventada.

No estamos poniendo en duda a Bitcoin, todo lo contrario, ponemos en duda el factor humano. Debido a no seguir unas mínimas buenas prácticas de seguridad, se cuentan en casi 1000 millones de dólares los bitcoins que se han robado. Así que nunca está de más prevenir.

De hecho, cualquiera que haya seguido la moneda desde sus inicios sabrá que no han sido pocos (más de 40) ni pequeños los “golpes” que se han dado en su corta historia, y todo, siempre debido a fallos humanos en grandes puntos de concentración de bitcoins.

No solo teniendo tus fondos en los monederos y cuentas de las casas de cambio corres el riesgo de perderlos

Al igual que en el mundo real, en la red todo es susceptible de ser hackeado por muy bien protegido que creas que está. No obstante, si sigues estas recomendaciones, se lo pondrás extremadamente difícil a todo aquel/la que tenga la intención de robarte.

## **1. Gestiona tus propias claves**

Este consejo es muy básico, pero a veces se nos olvida.

Debes ser muy (pero que muy) precavido (e inicialmente desconfiar) de

los servicios online donde almacenar bitcoins, sean del tipo que sean: monederos, casas de cambio, apuestas, ...

Analiza muy bien el servicio y su reputación antes de mandar ni un solo satoshi o decir a alguien que te los mande ahí.

Recuerda los casos anteriores de robos, todos tenían muy buena reputación. Incluso siendo sitios de confianza pueden ser comprometidos por un delincuente. Debes entender que en el momento en el que tu no tengas los bitcoins estos pueden desaparecer. Así que, en la medida de lo posible, ten tus bitcoins el mínimo tiempo en terceras

manos.

## **2. Mantén tu software actualizado**

Por regla general vas a usar un programa informático como monedero y cliente Bitcoin, y lo harás a través de tu ordenador o smartphome.

Es decir con este programa, almacenarás tus claves privadas y operarás con ellas a través para hacer movimientos de tus bitcoins.

Pues bien, en este caso preocupate de que todo lo que tu ordenador o teléfono móvil tiene está actualizado y libre de malware de cualquier tipo.

## **3. Cifra tus claves privadas**

Actualmente, cualquier programa de

monedero que se precie, va a crear tus claves privadas de forma automática. No todos siguen buenas prácticas en la creación de estas claves privadas, evitando que sea sencilla de replicar, pero los más conocidos si lo hacen.

Lo que es importante entender es que, una vez creadas, se guardan en tu dispositivo en texto plano. En algún fichero o base de datos interna.

No obstante, los mismos monederos suelen tener un proceso para cifrar la clave privada con una contraseña o “PIN”, de esa forma en el momento de hacer un envío te la pedirá, pero si alguien te roba las claves privadas deberá saber esa clave. Esto quiere

decir que tu clave privada se modifica en base a esa contraseña o PIN dejando de ser útiles tal cual.

Usar algo como una o varias palabras de diccionario o números tipo “123456”, es una muy muy mala idea.

Para hacerte la vida más fácil puedes utilizar gestores de contraseñas como [Lastpass](#), que son muy seguros si se usan bien y te ayudan a generar contraseñas fuertes y recordarlas corriendo riesgos mínimos.

#### **4. Usa doble autenticación**

¿Eres una persona que le gusta el riesgo y has depositado tus bitcoins en algún servicio web?

En este caso te recomendamos que, como mínimo, uses un segundo nivel de seguridad.

El factor de doble autenticación es un proceso que sirve para verificar tu identidad a la hora de acceder a un servicio web.

Parece increíble, pero casi no importa que uses contraseñas larguísimas o complejas hoy en día. El 99% de las contraseñas se roban a través de procesos de phishing.

Con el segundo factor de seguridad se evitaría que, si alguien obtiene tu contraseña, no pueda acceder a tu cuenta, pues necesita una segunda clave única proporcionada en ese mismo

momento a través de una vía alternativa.

Por ejemplo, podrías utilizar herramientas como [Authy](#) o [Google Authenticator](#), son gratis, multiplataforma y es compatible con muchos otros servicios como Twitter o Dropbox, además de los servicios de Google.

Una vez sincronizado con el servicio, tras la contraseña te pedirá un código único que cambia cada 60 segundos. Este código te lo entrega el programa que uses para gestionar este segundo factor de seguridad. De esta forma si alguien se hace con tu contraseña no podrá mover los bitcoins, pues no tiene

ese código único.

No te da una seguridad infalible, pues el delincuente que tenga acceso a esta segunda clave que se genera podría acceder igualmente, pero aumenta muchísimo tu seguridad debido a la complejidad de que esto ocurra.

## **5. Haz copias de seguridad**

Si utilizas un monedero que no esté alojado en algún servicio online es conveniente que hagas diferentes copias de seguridad almacenadas en distintos lugares.

Una vez has hecho estas copias, encriptalas con otros servicios para

hacerlas prácticamente incorruptibles. Puedes guardar las copias en servicios de almacenamiento en la nube, pendrives, tarjetas SD, etc.

Tener copias de seguridad es importante siempre, y más para tu dinero, pero también lo es cuidar de ellas. Supongo que no querrás ser como James Howells, quien tiró a la basura un disco duro con 7500 bitcoins (los cuales llegaron a valer casi 8 millones de dólares) y aún está recorriendo basureros de su país para intentar localizarlo.

## **7. Manténlos fuera de la red**

Este es uno de los procesos más

complejos pero puede añadir una capa muy grande de seguridad.

La idea es simple: Si hay que evitar que nadie pueda robarme mis claves privadas, las almacenaré en un lugar desconectado de internet.

Para ello podemos diferenciar en 3 tipos de almacenar las claves:

**Paper wallets:** Consiste en imprimir la clave en uno o varios papeles y almacenarlos en lugares seguros.

**Brain wallets:** Memorizar la clave privada. Para ello pueden usarse claves nemotécnicas usadas en monederos de tipo HD.

**Hardware:** Son dispositivos físicos que almacenan tus claves y jamás salen de

ellos. Para ello se conectan por USB/OTG y tu monedero les pasa la transacción para que el dispositivo lo firme con la clave privada.

## **Piensa en tu testamento**

No queremos ser fatalistas, pero es importante tener en cuenta todas las posibilidades. Un exceso de seguridad sin un plan B puede ser peligroso. En caso de un fatal acontecimiento, los bitcoins que has ido almacenando a lo largo de una vida pueden quedar totalmente inaccesibles, incluso para tus familiares, debido a que el lugar donde guardas estas claves privadas (y las contraseñas para descifrar las claves si

las has cifrado) sea tan privado que nadie, al margen de ti, lo sepa.

Este es un punto controvertido, pues esa misma gente en la que dejas tu confianza a modo de plan B podría ser quien te robe.

En este caso puede ser buena idea usar el monedero multifirma donde puedes crear una configuración de copias de claves guardadas en cajas fuerte o lugares que tras tu muerte serán heredados.

Una de las grandes revoluciones en esta línea son los Smart Contracts, que serán capaces de enviar tus bitcoins a quien tu decidas una vez fallezcas.

# Historia de los Exchanges Bitcoin

En febrero de 2010, dwdollar creó un portal llamado Bitcoin Market en el que se podían comprar y vender bitcoins de persona a persona incluyendo sistemas de pago como PayPal convirtiéndose así en una de las primeras referencias en la compra y venta de BTC conocidas hasta la actualidad. El día 4 de junio de 2011 se dejó de ofrecer soporte a PayPal en Bitcoin Market por el fraude que hacían algunos usuarios reclamando que no recibían nada a cambio de lo que habían pagado por los bitcoins.

El gran conocido: MTGox

Sí... MTGox... todo bitcoiner conocerá esta casa de cambio que llegó a ser de las más utilizadas hasta la llegada de otras páginas como Bitstamp.

Nacido en julio de 2010 de la mano de Jed McCaleb y vendido el 6 de marzo a Tibanne Co. Ltd.

**¿Por qué debería conocerse?**

Sus problemas de seguridad estaban en la orden del día. Empezando el 19 de junio de 2011 con una importante brecha de seguridad que forzó el cierre de la operativa en MTGox por 7 días al verse comprometida la base de datos de usuarios con nombres de usuario, direcciones de correo electrónico y

hashes de más de 6000 cuentas.

Los atacantes pudieron acceder también a una cuenta de administrador y ejecutar órdenes de venta de cientos de miles de BitCoin, bajando el precio desde los 17.51 dólares hasta 0.01\$ conllevando también el robo de los balances de unas 600 cuentas de MyBitcoin (de las primeras eWallet de la historia de bitcoin) que mantenían el mismo usuario y contraseña que en MTGox.

## **Pérdidas en Exchange BitCoin**

El tiempo pasó y los ataques persistían en exchanges como los que te citamos cronológicamente:

Bitomat, exchange polaco tercero en

volumen que perdió 17000 BTC de sus usuarios.

120000 Bitcoins de MyBitcoin, valorados en ese momento en unos 2 millones de dólares.

100000 dólares perdidos por el exchange TradeHill que provocaron su cierre inminente. En febrero de 2012 era el segundo exchange más importante. Bitcoinica pierde el 11 de mayo de 2012 más de 18000 Bitcoins con un valor de unos 90000\$.

2012 fue un año duro para las empresas y casas de cambio BitCoin, pues los robos seguían aconteciendo y es que en septiembre de 2012 el cuarto mayor exchange estadounidense Bitfloor sufrió

un ataque que supuso la pérdida de 24000 Bitcoins valorados en ese momento en unos 250000\$ causando el cese de toda su operativa.

Unos meses después y pese a tanto movimiento en lo que a robos se refiere, el precio de un BitCoin cotizaba en los 30\$ de nuevo desde 2011 estableciendo un máximo o “all time high” el 28 de febrero en MTGox.

El precio seguía progresando hasta que se llegó al billón de capitalización el 28 de marzo de 2013, pasando los 100\$ en abril y empezando una de las conocidas como primeras burbujas en la cotización que lo llevó hasta los 266\$ por bitcoin.

## ¿Qué fue lo siguiente?

La llegada a los 1000\$/BTC en noviembre de 2013. El momento de gran euforia entre toda la comunidad y con pocos imaginando lo que sucedería tan sólo 3 meses después. MTGox detuvo los retiros el 7 de febrero de 2014 por insolvencia después de un robo sin detectar que se acontecía desde 2011.

Antes comentábamos que MTGox era quizá el exchange más conocido y es que sus pérdidas estaban valoradas en medio billón de dólares en el momento de su cierre, convirtiéndose así en la mayor pérdida de Bitcoins.

## **Panorama actual**

¡No todo son robos o negatividad..!  
Bitcoin se ha ido asentando con el paso de los años y su capitalización ya supera los 114 Billones de dólares con un precio de más de \$6700 a día 10 de abril de 2018 y con distintos exchanges establecidos a nivel oriental y occidental.

**Entre los más importantes encontrarás los que te citamos a continuación.**

# Exchanges Occidentales

## **Kraken**

Uno de los exchanges más nuevos pero con un nivel de crecimiento impresionante que le permite disponer de un volumen de más de 18.497 BTC diarios.

– Información sobre Kraken:

<https://www.kraken.com/>

## **Bitfinex**

Bitfinex es también uno de los exchanges más comunes a nivel europeo que ganó

una importante cuota de usuarios después del ataque que sufrió Bitstamp a principios de 2015. Volumen diario aproximado de 56.238 BTC

– Información sobre Bitfinex:

<https://www.bitfinex.com/>

## **Bitstamp**

Un clásico y alternativa a MTGox antes de sus peores momentos. El soporte de grandes inversores y su posición como primer exchange regulado en Europa le permiten seguir siendo uno de los exchanges de la vieja escuela pese a haber tenido también algunos problemas en el pasado con un volumen actualmente de más de 12.681 BTC cada

24h.

– Información sobre Bitstamp:

<https://www.bitstamp.net/>

# Exchanges Orientales

Los exchanges orientales también tienen un papel importante en el mercado de trading BitCoin, el volumen que mueven a diario pese a las acusaciones sobre la utilización de bots para generarlo es muy superior al de los demás exchanges y suelen ser una referencia para grupos de traders o analistas interesados en la cotización de bitcoin.

¿Todavía no has oído hablar sobre ninguno de ellos? ¡No te preocupes!

## **OKcoin**

Fundado en el año 2013, sus mercados de futuros le posicionan como el primer

exchange en volumen tanto oriental como internacional con más de 1 millón de Bitcoins movidos al día en mercados como BTC/CNY y LTC/CNY. Litecoin es una criptomoneda con un nivel de trading elevado en Oriente. Dispone de dos portales. Uno dónde el volumen principal se desarrolla en USD y otro en el que CNY es la moneda FIAT predominante.

– Información sobre OKCoin:

<https://www.okcoin.com/>

## **Huobi**

Fundado en septiembre de 2013, es el segundo exchange a nivel de volumen en la actualidad con unos más de 115.797

BTC movidos cada 24h. Sus mercados predominantes también son los pares BTC/CNY y LTC/CNY.

– Información sobre Huobi:

<http://www.huobi.com/>

## **BTCChina**

Este exchange no está exactamente en la tercera posición a nivel oriental en lo que a volumen se refiere ya que en la actualidad mueve unos 6.796 BTC de volumen a diario, pero su base de usuarios es sólida al estar operativo desde junio de 2011. Como en todo exchange Oriental, el volumen principal se desarrolla entre los mercados BTC/CNY y LTC/CNY.

– Información sobre BTCChina:  
<https://www.btcc.com/>

# ¿Qué es Minar Bitcoins?

En cualquier sistema monetario tradicional, los gobiernos simplemente imprimen más dinero cuando lo necesitan.

En lo que respecta a Bitcoin, este no se crea, sino que se descubre. Para entenderlo mejor vamos a ver el siguiente vídeo:

**Haz clic sobre la  
imagen para  
visualizarlo**



Miles de ordenadores de todo el mundo “minan” Bitcoins compitiendo unos con otros.

Los mineros obtienen los Bitcoins como recompensa a la resolución de un problema matemático en el que cada 10 minutos compiten miles de nodos siendo la red de computación más potente que hoy en día existe (Si, por encima incluso que NSA o el todopoderoso Google).

Este reto matemático siempre es igual en su proceso pero las variables son diferentes y solo puede resolverse probando números al azar sin parar hasta dar con el resultado que se busca en ese momento. El primero que lo consiga se lleva la recompensa. Esto genera competencia y búsqueda de eficiencia mejorando los ordenadores para este objetivo, a los que llaman mineros.

# ¿Cómo funciona el minado?

La gente envía de forma constante Bitcoins de un lado a otro pero salvo que alguien registrase todas estas transacciones, nadie podría comprobar quién ha pagado qué en un momento determinado.

La red de Bitcoin gestiona esto dejando constancia de todas las transacciones llevadas a cabo en un periodo determinado en una lista, llamada bloque.

El trabajo de los mineros es confirmar

esas transacciones y escribirlas en el “libro mayor” (cadena de bloques)

Este “libro mayor” es una larga lista de bloques conocida como la “cadena de bloques”.

Puede utilizarse para explorar cualquier transacción que haya tenido lugar entre direcciones de Bitcoins en cualquier lugar.

Cada vez que se crea un nuevo bloque, se añade a la cadena, creando un lista cada vez mayor con todas las transacciones que se han hecho en toda la historia de la red de Bitcoin.

Una copia actualizada en tiempo real de los bloques se descarga en cada ordenador o nodo que esté aportando

poder computacional a la red.

Este libro mayor tiene que generar confianza y todo esto se sostiene de forma digital. ¿Cómo podemos asegurarnos de que la cadena de bloques permanece intacta y nadie la manipula?

Aquí es donde entran en juego los mineros.

Cuando se crea un bloque de transacciones, los mineros dan lugar a él siguiendo un proceso.

Cogen la información del bloque y le aplican una fórmula matemática, convirtiéndolo en algo diferente.

Esta nueva “pieza de información” es más corta y en apariencia es una secuencia de números y letras aleatoria

denominada técnicamente “hash”.

Este “hash” se almacena con el bloque, al final del mismo, en último lugar en la cadena en ese momento.

Los “hash” tienen algunas propiedades interesantes. Es fácil producir un “hash” de un conjunto de datos como un bloque de transacciones, pero es prácticamente imposible acceder a los datos simplemente con el “hash”.

Mientras que es muy fácil producir un “hash” de un gran conjunto de datos, cada uno es único.

Si cambias un único carácter del bloque, el “hash” cambiará por completo.

Los mineros no solo usan las

transacciones de un bloque para generar un “hash”. También se utilizan otros datos. Uno de estos datos es el “hash” del último bloque añadido a la cadena.

Debido a que el “hash” de cada bloque se produce utilizando el “hash” del bloque inmediatamente anterior, se convierte en una versión digital de un “sello de lacre”.

Confirmar que ese bloque y todo aquel que va a continuación es legítimo. Si intentases falsificar una transacción cambiando un bloque que ya había sido almacenado en la cadena, el “hash” de ese bloque cambiaría.

Si alguien comprobase la autenticidad

del bloque aplicando la función matemática encima, se encontrarían con que el “hash” sería distinto de aquel que ya está almacenado con ese bloque en la cadena y, como consecuencia, el bloque sería automáticamente identificado como falso.

## **Compitiendo por monedas**

De esta manera los mineros “sellan” los bloques. Todos compiten entre ellos para hacer esto, utilizando software escrito específicamente para minar bloques.

Cada vez que alguien crea un “hash” con éxito, se lleva una recompensa de 12,5 bitcoins, la cadena de bloques se

actualiza y todo el mundo en la red es notificado con ello.

Ese es el incentivo para seguir minando y permitir que se sigan llevando a cabo transacciones.

El problema es que es muy fácil producir un “hash” directamente a partir de un conjunto de datos.

Ya que para un ordenador resulta muy fácil hacer esto, la red de Bitcoin ha de hacerlo más difícil, ya que de otra manera todo el mundo estaría creando “hashes” de centenares de bloques de transacciones cada segundo y todos los bitcoins se minarían en minutos.

El protocolo de Bitcoin simplemente no

aceptaría ningún “hash” antiguo.  
Requiere que el “hash” de cada bloque sea de una manera determinada, debiendo tener un número de ceros determinado al principio.

No hay manera de saber cómo va a ser un “hash” antes de producirlo y, tan pronto se incluya un nuevo dato, el “hash” será totalmente diferente.

Se supone que los mineros no interaccionan con los datos referentes a transacciones que hay dentro de cada bloque, pero deben cambiar los datos que están utilizando para crear un “hash” diferente.

Hacen esto utilizando otro trozo de

información aleatorio que se conoce como “nonce”, que se utiliza con los datos de la transacción para crear un “hash”.

Si el “hash” no se ajusta al formato requerido, el “nonce” se cambia y se prueba de nuevo creando un nuevo hash otra vez.

Puede conllevar varios intentos encontrar un “nonce” que funcione y todos los mineros de la red están intentando hacerlo al mismo tiempo. De hecho lleva millones de intentos, por miles de ordenadores que todos intentan dar con el numero que devuelva el patrón que en ese momento se está pidiendo. Así es como los mineros se

“ganan su sustento”.

De momento aquí termina esta guía básica sobre los primeros pasos que debes conocer sobre Bitcoin y Criptomonedas. Indudablemente no es toda la información que quiero compartir contigo, hay MÁS, muchísimo MÁS

Pero si te parece vamos hacerlo paso a paso, no te preocupes. Mi compromiso contigo es guiarte en todo el proceso para que TÚ TAMBIÉN empieces a generar ingresos gracias al BitCoin y las criptomonedas.

Lo importante ahora es saber si hasta ahora tienes preguntas sobre lo que

hemos recorrido en estas líneas.  
Espero tus comentarios,

Saludos

Richard García

WhatsApp: [+34678784359](https://wa.me/34678784359)