**WHAT IS BITCOIN – HISTORY, HOW IT WORKS, PROS & CONS**

***TOPICS***

1. What is Bitcoin
2. History of Bitcoin
3. How it works ( Blockchain)
4. Pros and Cons

***STRUCTURE***

* Heading
* Abstract
* Introduction
* Couple Headings
* Conclusion

1. ***WHAT IS BITCOIN***

**Bitcoin** es una moneda, como el euro o el dólar estadounidense, que sirve para intercambiar bienes y servicios. Sin embargo, a diferencia de otras monedas, Bitcoin **es una divisa electrónica** que presenta novedosas características y destaca por su eficiencia, seguridad y facilidad de intercambio.

Su mayor diferencia frente al resto de monedas, se trata de una moneda descentralizada, por lo que nadie la controla. Bitcoin no tiene un emisor central como los dólares o los euros, la criptomoneda es producida por las personas y empresas de alrededor del mundo dedicando gran cantidad de recursos a la minería.

#### **Veamos algunas características de introducción a Bitcoin:**

* No pertenece a ningún Estado o país y puede usarse en todo el mundo por igual.
* Puedes [comprar bitcoins](https://goo.gl/jjmjgd) con euros u otras divisas y viceversa, como cualquier moneda.
* No hay intermediarios: Las transacciones se hacen directamente de persona a persona.
* **Es descentralizada**: no es controlada por ningún Estado, banco, institución financiera o empresa.
* Es imposible su falsificación o duplicación gracias a un sofisticado sistema criptográfico.
* Las transacciones son irreversibles.
* No es necesario revelar tu identidad al hacer negocios y preserva tu privacidad.
* El dinero te pertenece al 100%; no puede ser intervenido por nadie ni las cuentas pueden ser congeladas.

La Red Bitcoin está basado en un **sistema “*peer to peer”***o de usuario a usuario que ha permitido romper con un problema en todos los medios de pago anteriores, la necesidad de una tercera parte. Antes de la invención de Bitcoin, cuando quería realizar un pago online, se tenían que recurrir a plataformas como Paypal, Neteller, Bancos, etc para realizar los pagos.

***2.HISTORY OF BITCOIN***

Bitcoin nació en 2009 como un protocolo informático y una red P2P que buscaba ofrecer alternativas de pago al margen de las monedas corrientes. **Esta moneda virtual no estaría apoyada por ningún gobierno**. Por ello, las transferencias en este formato se hacen más difíciles de rastrear y se convierten en un atractivo para las actividades ilegales.

Por otro lado, y por cuestiones informáticas, **el número total de Bitcoins en circulación no puede superar los 21 millones**. Esto ha hecho que el propio Bitcoin se convierta en un producto con valor intrínseco, al ser un bien escaso.

Desde su creación, muchas grandes empresas como Microsoft, Dell, Reddit o Virgin Galactic han aceptado el pago con Bitcoin. **En 2011 Wikileaks pidió donativos en esta moneda**, dado el bloqueo que había sufrido por empresas de crédito como VISA, MasterCard y PayPal.

Un año más tarde, en 2012 se creó la Bitcoin Foundation, buscando **estandarizar el uso del Bitcoin** e intentando mantenerlo libre y fuera de las manos de los gobiernos.

Llegamos a enero de 2015 Una empresa española, Bit2Me ofrece**por primera vez cambio de Bitcoins a euros**. A partir de entonces, el uso de bitcoins en la UE empezó a legislarse. En España se consideró que su uso estaba exento de IVA a principios de ese 2015. Para finales del año, el uso en toda la UE se consideró exento de pago de IVA.

Su uso se ha extendido, tanto en los mercados financieros como en los mercados criminales. Un ejemplo de esto último: en el reciente [**ciberataque a escala global**](https://www.tuexperto.com/2017/05/12/el-virus-wannacry-se-extiende-por-todo-el-mundo/) usando el virus WannaCry, l**os hackers responsables exigieron un pago en Bitcoins** para liberar los ordenadores “secuestrados”. En concreto, 17 céntimos de Bitcoin por cada equipo.

Estos usos fraudulentos, así como los usos para blanquear dinero, son los **grandes retos y amenazas a los que se tiene que enfrentar** esta criptomoneda. Es el precio del código abierto y la libertad absoluta.

Tras una secuencia de subidas históricas, algunos mineros y start ups deciden separarse de los desarrolladores originales creando lo que se llama el [hard fork](https://bitcoinclassic.com/). Bitcoin se convierte en **Bitcoin Cash** y nacen**Bitcoin Core, Bitcoin Classic y Bitcoin Unlimited**.

A lo largo del año, bitcoin no para de marcar altos históricos, **superando los 3.400 dólares por moneda el 7 de agosto** y un valor total de 5.000 millones. Esta separación noparece haber dañado la confianza en la moneda sino más bien fortalecerla.

China ha [**anunciado**](http://www.rewisor.com/china-primer-pais-criptomoneda/)la creación de su propia criptomoneda y los gobiernos de India, australia y muchos más están estudiando cómo incluirla en sus infraestructuras.

***3.HOW IT WORKS***

El funcionamiento de Bitcoin se puede expresar en 3 grandes bloques.

**Balances - cadena de bloques**

La cadena de bloques o "block chain" es una **contabilidad pública compartida** en la que se basa toda la red Bitcoin. Todas las transacciones confirmadas se incluyen en la cadena de bloques. De esta manera los monederos Bitcoin pueden calcular su saldo gastable y las nuevas transacciones pueden ser verificadas, asegurando que el cobro se esta haciendo al que realiza el pago. La integridad y el orden cronológico de la cadena de bloques se hacen cumplir con criptografía.

**Transacciones - llaves privadas**

Una transacción es **una transferencia de valores entre monederos Bitcoin** que será incluida en la cadena de bloques. Los monederos Bitcoin disponen de un fragmento secreto llamado *clave privada*, utilizada para firmar las operaciones, proporcionando una prueba matemática de que la transacción está hecha por el propietario del monedero. La *firma* también evita que la transacción no sea alterada por alguien una vez ésta ha sido emitida. Todas las transacciones son difundidas entre los usuarios y por lo general empiezan a ser confirmadas por la red en los 10 minutos siguientes a través de un proceso llamado *minería*.

**Procesamiento - minería**

La minería es un **sistema de consenso distribuido** que se utiliza para *confirmar* las transacciones pendientes a ser incluidas en la cadena de bloques. Hace cumplir un orden cronológico en la cadena de bloques, protege la neutralidad de la red y permite un acuerde entre todos los equipos sobre el estado del sistema. Para confirmar las transacciones, deberán ser empacadas ​​en un *bloque* que se ajuste a estrictas normas de cifrado y que será verificado por la red. Estas normas impiden que cualquier bloque anterior se modifique, ya que hacerlo invalidaría todos los bloques siguientes. La minería también crea el equivalente a una lotería competitiva que impide que cualquier persona pueda fácilmente añadir nuevos bloques consecutivamente en la cadena de bloques. De esta manera, ninguna persona puede controlar lo que está incluido en la cadena de bloques o reemplazar partes de la cadena de bloques para revertir sus propios gastos.

***4.PROSS & CONS***

**ANONIMATO VS ILEGALIDAD**

La red Bitcoin está descentralizada, lo que significa que todo el mundo que accede a ella goza de anonimato. Sin embargo, esto también tiene un aspecto negativo. Debido a su anonimato, el Bitcoin es utilizado por vendedores de armas y de drogas así como por terroristas. Por esta razón no se ha determinado la situación legal de la criptomoneda.

**Transparencia de las transferencias vs. Amenaza de pirateo**

Siempre es posible hacer un seguimiento de sus transacciones en la página web blockchain.info. Sin embargo, todo está alojado en la red, por lo que podría perder fácilmente su dinero.

**Dinero alternativo vs. Criptomonedas alternativas**

El Bitcoin ha registrado un gran crecimiento desde su aparición. Sin embargo, sus competidores están alcanzando nuevos récords, así que tal vez el Bitcoin no sea la mejor apuesta para los inversores en criptomonedas.

**Bajas comisiones vs. Volatilidad**

En comparación con otros pagos electrónicos, las comisiones de la red de Bitcoins son más bajas. Sin embargo, también hay que tener en cuenta la alta volatilidad de la criptomoneda, que puede caer desde los 2.000 $ o 3.000 $ hasta los 500 $ en un solo día.

**Ausencia de un regulador vs. Falta de garantías**

El Bitcoin no pertenece a nadie, lo que significa que nadie puede controlarlo.