

CURSO DE BITCOIN FUNDAMENTOS

INSTITUTO BME 2016

Índice

0. OBJETIVO DEL CURSO
1. ¿Qué son las monedas virtuales?
2. Historia del Bitcoin
3. ¿QUÉ ES BITCOIN?
4. DIFERENCIAS ENTRE BITCOIN, ORO Y DOLAR
5. ¿Cómo usar Bitcoin o cualquier otra criptomoneda?
6. ¿Cómo obtener Bitcoins?
7. ¿CÓMO COMPRAR Y VENDER BITCOINS?
8. ¿Cómo aceptar pagos en Bitcoin?
9. ¿QUÉ ES LA MINERÍA DE BITCOINS (CRIPTOMONEDAS)?
10. ¿CÓMO MINAR CRIPTOMONEDAS?
11. Usos del Bitcoin Como Tecnología
12. Bitcoin vs otras Criptomonedas.
13. ¿Qué es Ethereum?
14. Popularidad del Bitcoin
15. ¿Cómo es la regulación de Bitcoin en el Mundo?
16. Algunas webs relevantes en el mundo Bitcoin.

LAVADO DE CELEBRO DEL MUNDO FIAT

ECONOMIA VIRTUAL

SER FAN DEL BITCOIN

HACEROS BITCOINERS

1. ¿Qué son las monedas virtuales?

Las monedas virtuales son un “medio digital de intercambio”, es decir, es dinero virtual, y puesto que está relativamente aceptado, se puede utilizar para comprar y vender productos y servicios.

La mayor diferencia con respecto a las monedas tradicionales es que no están sujetas a la supervisión y control de ningún gobierno o emisor central, como el Banco Central Europeo, en el caso del euro.

La moneda virtual más popular, y la primera totalmente implementada, ha sido el Bitcoin.

1. ¿Qué son las monedas virtuales?

¿Qué es una moneda virtual?

El Banco central Europeo (BCE) definió en 2012 ‘moneda virtual’ como “un tipo de dinero no regulado, digital, que se emite y por lo general está controlado por sus desarrolladores, y que es utilizado y aceptado entre los miembros de una comunidad virtual específica.

¿Qué es una moneda digital?

Moneda digital, sin embargo, es una forma de moneda virtual que se crea y se almacena electrónicamente. Las criptomonedas son un tipo de moneda digital, pero no las únicas. Las criptomonedas son, un subconjunto de las monedas digitales basadas en la criptografía, en algoritmos matemáticos.

El prefijo cripto, proviene de la palabra griega kruptos, que significa oculto, secreto. Criptografía es el estudio de métodos de encriptación de información, principalmente utilizados para enviar un mensaje de manera segura y privada, y para la seguridad y autentificación de datos.

1. ¿Qué son las monedas virtuales?

Otras definiciones de criptomoneda

El diccionario de Oxford, incluyó la definición de su traducción en inglés (cryptocurrency): “Una moneda digital que emplea técnicas de cifrado para reglamentar la generación de unidades de moneda y verificar la transferencia de fondos, y que opera de forma independiente de un banco central”.

El diccionario de Cambridge, por su parte, ha definido con estos términos la palabra inglesa: “Una moneda digital producida por una red pública en lugar de cualquier gobierno, que utiliza la criptografía para asegurar que los pagos se envían y reciben de forma segura.”

1. ¿Qué son las monedas virtuales?

El periódico digital especializado en Bitcoin [Coindesk](#) define el término criptomoneda como: “***Una forma de moneda basada únicamente en las matemáticas. En lugar de la moneda fiduciaria, que se imprime, una criptomoneda se produce mediante la resolución de problemas matemáticos basados en criptografía.***”

Wikipedia la define como: “***Una criptomoneda es un medio de intercambio que utilizan la criptografía para asegurar las transacciones y controlar la creación de nuevas unidades.***”

Las criptomonedas están respaldados por las matemáticas, lo que hace que no pueda ajustarse por un solo grupo o persona. Las criptomonedas no están vinculadas a la disponibilidad de los bienes físicos, como en el caso del oro.

1. ¿Qué son las monedas virtuales?

La moneda virtual es dinero pero que no podemos ver ni palpar, es decir, que está dentro de un software de un dispositivo tecnológico como puede ser un móvil o un ordenador que se le denomina "billetera virtual" o "monedero virtual".

Las características principales de este dinero virtual es que ningún gobierno tiene control de la información de las transacciones que se realizan, todas las transacciones se recogen la cadena de bloques <https://blockchain.info/> y las comisiones que se pagan son mínimas comparadas con otros servicios de envíos de dinero como Paypal.

2. Historia del Bitcoin

- Oro desde el origen de los tiempos.
- Monedas indexadas al Patrón Oro.
- “Dinero Fiat” que es de curso legal por decreto y que a partir de 1971 sustituye al “patrón oro” esto hace que los gobiernos puedan imprimir más dinero de que oro disponen lo que provoca Inflación y devaluación de la moneda. El dinero fiat esta sujeto a decisiones que quedan en manos del banco central o gobierno donde los intercambios monetarios están centralizados.

2. Historia del Bitcoin

- En 2008 aparece un artículo sobre Bitcoin elaborado por Satoshi Nakamoto BTC / XBT (Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario)
- Donde se definen:
 - Las bases de la moneda.
 - Algoritmos de funcionamiento.
 - Tasa de “impresión” de la moneda.
 - Descentralización de las transacciones
- En 2009 surge la primera implementación de un cliente Bitcoin.



2. Historia del Bitcoin

El 3 de enero de 2009, Satoshi lanzó la primera red descentralizada con tecnología Bitcoin y creó en ésta la primera criptomoneda con la publicación de su Bloque Génesis: bitcoin (BTC).

A los días de su creación, Nakamoto habría realizado la primera transacción con bitcoins de la historia al enviar 10 BTC al ya difunto criptógrafo Hal Finney.

2. Historia del Bitcoin

Por lo tanto las monedas digitales no son muy antiguas, nacieron en 2008 y actualmente siguen saliendo nuevas monedas todos los días prácticamente (coinmarketcap.com).

El motivo principal de crear una moneda virtual es mejorar la velocidad y la practicidad de la transacción, en vez de andar circulando con dinero físico en la mano. Como desventaja es que es difícil extraer o convertir ese dinero, que es virtual, en dinero real de forma rápida y efectiva, ya que al ser muy nuevo este concepto de monedas electrónicas, todavía no se ha popularizado su uso, ojo ya tenemos tarjetas de crédito que pagan en dinero fiat y se alimentan de bitcoins.

El uso del bitcoin se está extendiendo mas en países “monetariamente conflictivos” (Rusia, China, Venezuela,...) que aquellos que no lo son tanto, no hay tanta necesidad de los mismos... de momento.

2. Historia del Bitcoin

Está bastante extendido que las monedas virtuales surgieron para poder realizar pagos sencillos por medio de billeteras virtuales mediante gadgets, aparatos, tecnológicos, por ejemplo para comprar o vender con el móvil. Por ejemplo, nos tomamos una cerveza en un bar que acepta bitcoins como medio de pago. Entonces, el camarero le diría al cliente el código de la billetera virtual al cual la persona debe enviar el dinero correspondiente. Una vez se certifique que llegó el dinero, el cliente se podría ir porque ya ha pagado. Para esto en realidad sirven las monedas virtuales simplemente para comprar y vender productos.

<https://coinmap.org/#/map/40.42894144/-3.68411064/16>

Pero lo cierto es que cada vez más se utilizan las monedas virtuales (sobre todo el bitcoin) para invertir ya que su precio suele crecer debido a la gran demanda que hay de este dinero. Cuando el bitcoin salió al mercado en 2009, una unidad costaba tan solo unos centavos de dólar. En la actualidad su valor fluctúa alrededor de los 600 dólares. La persona que compró y mantuvo bitcoins desde entonces hasta ahora tendrá mucho dinero. Esto es como depósito de valor => ahora mismo lo más interesante. ¿Bitcoin como experimento social?

2. Historia del Bitcoin MAPA DE EVENTOS

BITCOIN Timeline of important events



3. ¿QUÉ ES BITCOIN?

Bitcoin es una Tecnología de Contabilidad Distribuida (DLT, por Distributed Ledger Technology) o Blockchain, en la cual copias de registros contables son distribuidas y validadas por un proceso de consenso con múltiples usuarios (nodos) que verifican de forma independientemente los cambios en la contabilidad.

La DLT crea una plataforma que permite intercambios y registros seguros sin necesidad de intermediarios. El sistema de pago Bitcoin es la aplicación DLT más conocida, open ledger.

La Tecnología Bitcoin (DLT) consta de tres partes:

Criptografía.

Cadena de bloques (block chain)

Red de consenso distribuido (red p2p).

3. ¿QUÉ ES BITCOIN? ESTO ES LA BASE DEL MODELO.

- La criptografía provee un mecanismo para la codificación segura de las reglas del protocolo en el sistema y se utiliza para evitar manipulación, robo o introducción de información incorrecta en la plataforma, así como para la generación de firmas e identidades digitales encriptadas.
- La cadena de bloques es una base de datos pública y distribuida en la que se registran de forma segura todas las transacciones que se realizan en la red. Open Ledger
- El consenso distribuido es la actuación de los participantes de la red verificando y confirmando la certeza y unicidad de las transacciones para generar una verdad irrefutable sobre éstas en la red peer-to-peer (p2p).

3. ¿QUÉ ES BITCOIN?

Pero tambien, como hemos visto antes es una divisa. Una divisa P2P global diseñada para internet como:

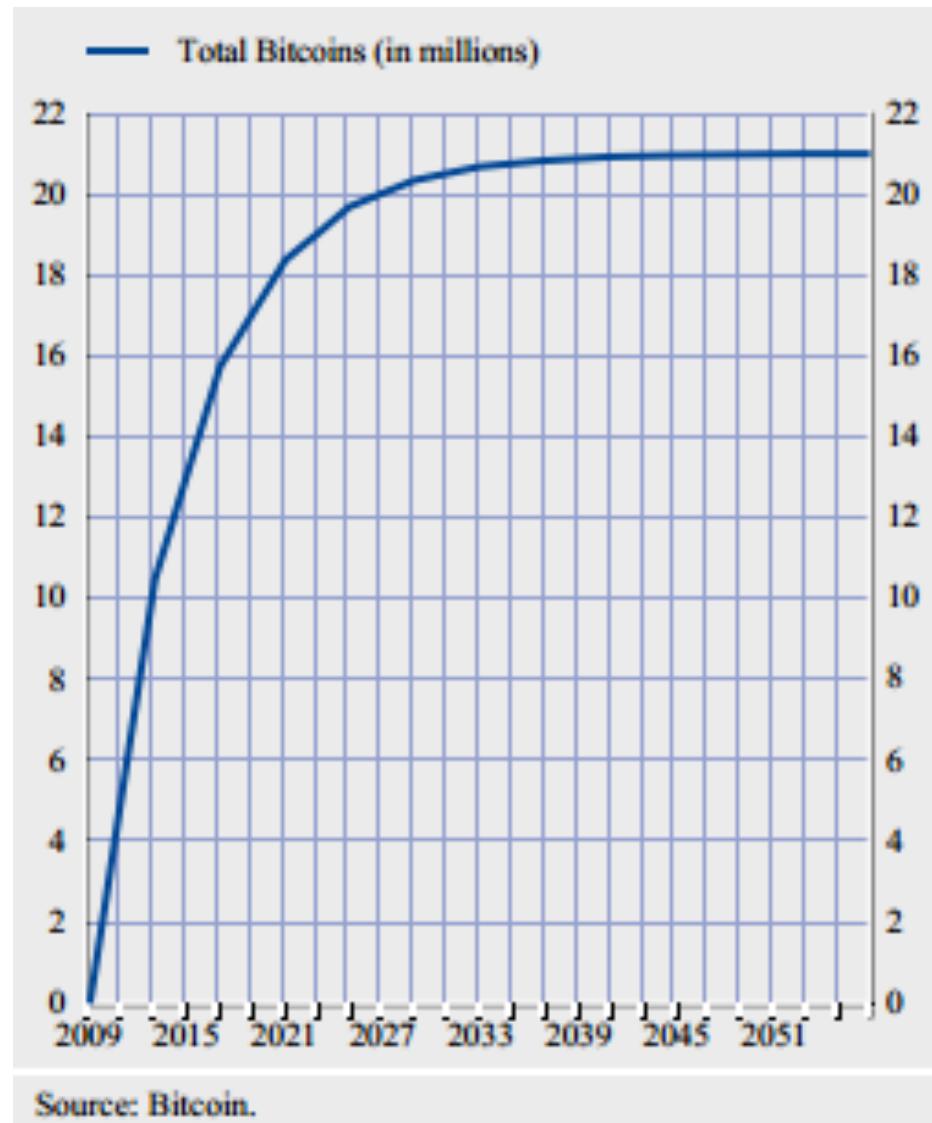
- Medio de pago
- Unidad de cuenta
- Depósito de valor

Deflacionaria por naturaleza. Sólo se crearán/minarán 21 millones de BTC entre su nacimiento 2,009 hasta el año 2,140 (8 decimales – 0,00000001 BTC = satoshi)

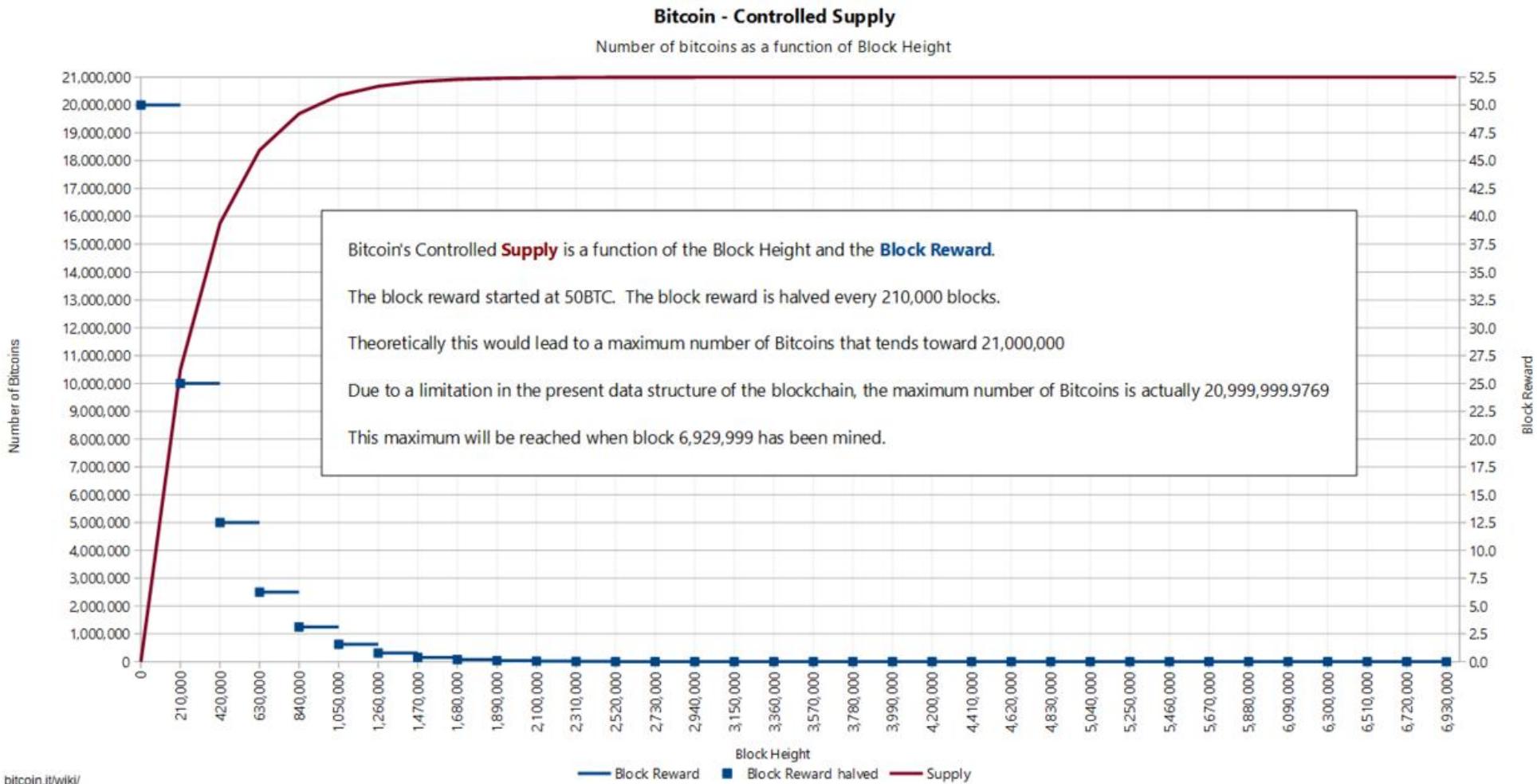
Libro de contabilidad transparente. Replicado por toda la red P2P y donde todas las transacciones pseudónimas se aprueban por CONSENSO.

3. ¿QUÉ ES BITCOIN?

- La tasa de generación de bitcoins está fijada en el algoritmo.
- Según aumenta la potencia de cálculo de la red se aumenta la complejidad – 1 bloque / 10 minutos.



3. ¿QUÉ ES BITCOIN?



3. ¿QUÉ ES BITCOIN? Unidades de medida

Tabla de medidas de Bitcoin:

- 1 BTC = 1 XBT = 1 bitcoin
- 1 BTC = 1,000 mBTC (millibitcoin) (1/1000 bitcoins = 0,001 BTC)
- 1 BTC = 1,000,000 μBTC (microbitcoin) (1/1.000.000 bitcoins = 0,000001 BTC)
- 1 BTC = 100,000,000 satoshis
- 1 mBTC = 100,000 satoshis = 1.000 μBTC
- 1 μBTC (microbitcoin) = 100 satoshis = 1 bit (1/1.000.000 bitcoins = 0,000001 BTC)
- 1 satoshi = 1/100.000.000 (0,00000001 BTC)

3. ¿QUÉ ES BITCOIN?

Sin ninguna autoridad central. Que emita, retire, devalúe o intervenga en su valor

Emitida por medio de RECOMPENSA. A cualquier nodo de la red (MINERO) que resuelva un puzzle matemático para validar las transacciones.

Controlada por programa abierto. Con unas reglas preestablecidas y cuyo código está disponible para revisión y mejora, que de hecho se actualiza periódicamente (Bitcoin Core Developers, BIP).

3. ¿QUÉ ES BITCOIN?

<https://pbs.twimg.com/media/CdhzUuCWEAlzFFw.jpg>

The infographic is titled "DEFINING BITCOIN" and includes the statement: "There is no shared definition of bitcoin, even often inside a single State."

BITCOIN IS: Commodity

In several countries, Bitcoin is taxed as property, & transactions are considered barter. This decision has been met with contention by some, but many investors have embraced this distinction, as it ultimately led to a legitimization of the technology, and to tax rates being cut in half.

Flags of Norway, USA, Australia, and Spain.

BITCOIN IS: Currency

Some have officially classified digital currency as alternative legal tender. As such, Bitcoin is regulated & taxed under the same laws governing each country's official currency.

Flags of the European Union, Germany, Finland, Canada, USA, and Argentina.

BITCOIN IS: Illegal

There are nations in which Bitcoin inspires fear within governments. In some cases, digital currency has been either over-regulated, or banned entirely. These laws have little effect on most users however, as many continue making use of Bitcoin and other similar coins in open rebellion of the law.

Flags of Turkmenistan, Iceland, Thailand, Ecuador, Bangladesh, and the Netherlands.

>Mainly Bitcoin is undefined because:

BITCOIN IS: Undefined

But at the same time, depending on THE APPLICABLE LAW and THE CONTEXT with a CONTINGENT APPROACH

BITCOIN IS NOT

- 1. MONEY
- 2. CURRENCY
- 3. COMMODITY
- 4. SECURITY
- 5. BARTER RIGHT
- 6. MEAN OF PAYMENT

BITCOIN IS

- 1. MONEY
- 2. CURRENCY
- 3. COMMODITY
- 4. SECURITY
- 5. BARTER RIGHT
- 6. MEAN OF PAYMENT

Flags of Belgium, Cyprus, Denmark, Greece, Italy, and Japan.

COINLEX, HolyTransaction

3. ¿QUÉ ES BITCOIN? Profundizamos en Criptografía 1

Criptografía BITCOIN

CONCEPTOS IMPORTANTES:

HASH

ALGORITMO DE ENCRYPTACION

CLAVE PRIVADA / CLAVE PUBLICA

Podemos pensar en la clave pública como si fuera el número de una cuenta bancaria y la clave privada como si fuera el PIN secreto. La clave pública es usada para recibir bitcoins, y la clave privada es usada para firmar las transacciones para gastar esos bitcoins.

3. ¿QUÉ ES BITCOIN? Profundizamos en Criptografía 2

- En el cliente bitcoin, se definen pares de claves pública/privada. Al crearse la cartera digital se generan dos claves digitales, una clave pública, dirección bitcoin o número de cuenta del usuario, que permite que se reciban depósitos en la cartera, y una clave privada del usuario dueño de la cartera que le permite transferir criptomonedas a otras carteras de otros usuarios.
- A partir de la privada se generan direcciones bitcoin. [Detalle](#).
- Las transacciones se realizan entre direcciones, que no están vinculadas a ninguna persona en concreto:
 - Las transacciones son públicas (se recogen en blockchain.info)
 - **Los exchanges o mercados pueden exigir identificación**
 - Propuesta base de datos centralizada de tenedores de bitcoin

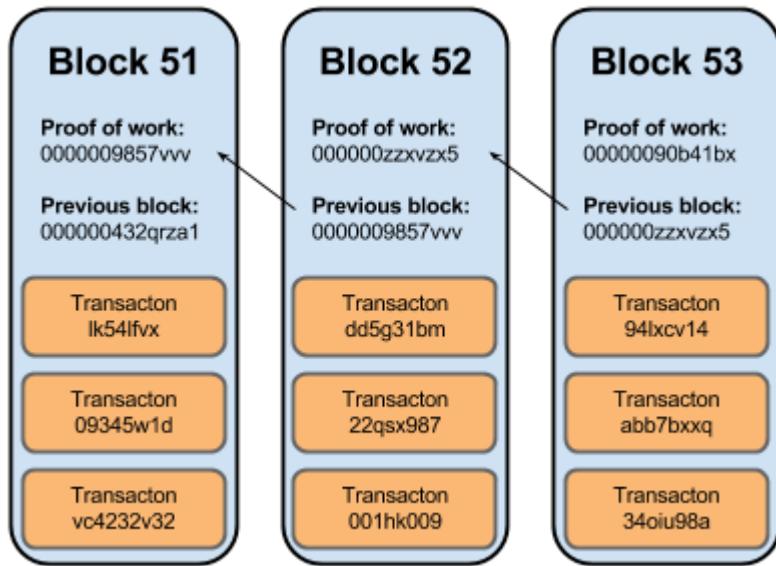
3. ¿QUÉ ES BITCOIN? Profundizamos en Criptografía 3



3. ¿QUÉ ES BITCOIN? Profundizamos en Criptografía 4

- Como tal entonces un bitcoin es un apunte contable, que indica que en una dirección, hay una cantidad de dinero.
- Estos apuntes contables se inscriben en bloques:
 - Se almacenan transacciones.
 - Un valor que “resuelve” el bloque.
 - El hash del bloque anterior
- De este modo, los bloques quedan enlazados, formando una cadena de bloques: Blockchain
 - Cadena contiene todas las transacciones
 - El tamaño del blockchain se incrementa cada 10 minutos con nuevos bloques. <https://blockchain.info/>

3. ¿QUÉ ES BITCOIN? Vision de cadena de Bloques

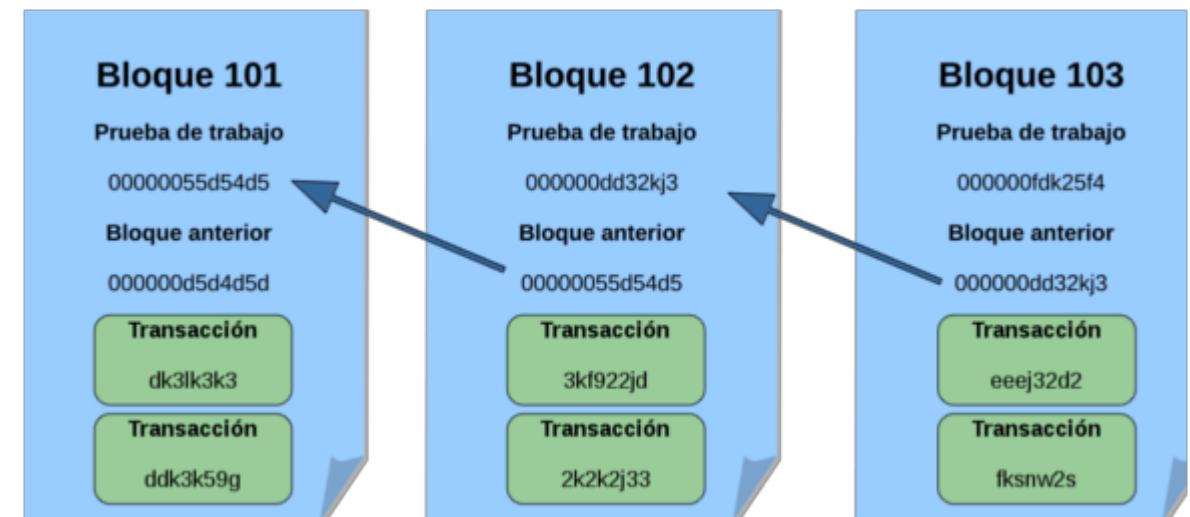


CADENA DE BLOQUES

Visible para todos

No se puede cambiar

No se puede borrar



3. ¿QUÉ ES BITCOIN? P2P

RED P2P:

- Operaciones entre pares, iguales.
- Pagos en todo el mundo
- Comisiones bajas o inexistentes

Bitcoin usa tecnología peer-to-peer o entre pares para operar sin una autoridad central o bancos; la gestión de las transacciones y la emisión de bitcoins es llevada a cabo de forma colectiva por la red. **"Bitcoin es de código abierto; su diseño es público, nadie es dueño o controla Bitcoin y todo el mundo puede participar."**



Todas las nuevas propiedades que tiene Bitcoin permite usos interesantes no contemplados por ningún sistema de pagos anterior. P2P <> SWIFT

3. ¿QUÉ ES BITCOIN? P2P

Características de las redes P2P:

- Escalabilidad. Con un uso cada vez más extendido de Internet, las redes P2P tienen un alcance mundial con cientos de millones de usuarios potenciales. En general, lo deseable es que cuantos más nodos estén conectados a una red P2P, mejor será su funcionamiento. Así, cuando los nodos llegan y comparten sus propios recursos, los recursos totales del sistema aumentan. Esto es diferente en una arquitectura del modo servidor-cliente con un sistema fijo de servidores, en los cuales la adición de clientes podría significar una transferencia de datos más lenta para todos los usuarios. Las redes P2P están basadas en código abierto que les permite ser flexibles.
- Robustez. La naturaleza distribuida de estas redes también incrementa la robustez ya que permite encontrar la información sin hacer peticiones a un servidor centralizado.
- Descentralización. Estas redes por definición son descentralizadas y todos los nodos son iguales. Ningún nodo es imprescindible para el uso de la red.
- Distribución de costes entre los usuarios. Se comparten o donan recursos a cambio de recursos. Según la aplicación de la red, los recursos pueden ser archivos, ancho de banda, ciclos de proceso o almacenamiento de disco.

3. ¿QUÉ ES BITCOIN? Desarrollo bitcoin, resumen

Satoshi Nakamoto abandonó el proyecto y lo dejó en manos de un grupo de desarrolladores que actualmente se conocen como Bitcoin Core. A pesar de ser ellos quienes dan la última palabra sobre qué se añade o elimina del código de Bitcoin, cualquier desarrollador puede colaborar con el proyecto y proponer sus códigos de mejora a través del repositorio en [GitHub](#). **APOYO DEL MIT PARA EL DESARROLLO.** <https://bitcoincore.org/>

<http://criptonoticias.com/eventos/mit-media-lab-y-w3c-organizan-taller-sobre-blockchain-para-discutir-possibles-estandares-de-trabajo/>

<http://criptonoticias.com/eventos/instituto-de-tecnologia-de-massachusetts-conferencia-bitcoin/>

<http://www.diariobitcoin.com/index.php/2015/04/23/mit-incorpora-a-desarrolladores-del-nucleo-bitcoin-a-su-iniciativa-de-una-nueva-moneda-digital/>

Resumiendo la criptomoneda bitcoin (BTC), por la que más se conoce a la tecnología, es una moneda digital descentralizada que se crea, se transfiere y se guarda de manera electrónica y se protege criptográficamente. Podría decirse que es la moneda de internet, efectivo digital.

3. ¿QUÉ ES BITCOIN? Desarrollo bitcoin, resumen

La descentralización de bitcoin se debe a que el control sobre la emisión (creación) de monedas se ejerce a través de reglas matemáticas que están programadas en el protocolo y que pueden ser cambiadas, únicamente, mediante el proceso de consenso de la red p2p. **No existe ningún organismo gubernamental o financiero que establezca control sobre la moneda.**

A diferencia de como sucede con el dinero físico o fiduciario (el euro, el dólar, el yuan, el rublo, etcétera), las criptomonedas no se imprimen. Los bitcoins, y otras monedas criptográficas, son creados por personas a través de computadoras que resuelven determinados problemas matemáticos para confirmar las transacciones que los usuarios de la red realizan y por lo que son recompensados en dicha moneda, proceso que se conoce como minería de bitcoins.

Para manejar bitcoin, o cualquier otra criptomoneda, es necesario crear una cartera o monedero digital, una aplicación en línea para computadoras, teléfonos móviles o tablets que permite guardar, enviar y recibir monedas digitales.

Comúnmente se utilizan las siguientes distinciones: Bitcoin, con B mayúscula, para referirse a la tecnología o a la red, y bitcoin, con b minúscula, para referirse a unidades de la moneda.

4. DIFERENCIAS ENTRE BITCOIN, ORO Y DOLAR

Aristóteles definió las características que tenía que cumplir el dinero para serlo, éstas son:

- Escaso
- Duradero
- Homogéneo
- Divisible
- Transportable
- Almacenable
- Difícil de falsificar

Revisamos oro, Bitcoin y dólar (como la moneda fiat de mayor duración hasta el momento).

4. DIFERENCIAS ENTRE BITCOIN, ORO Y DOLAR

Algunas de las diferencias entre el Bitcoin, el oro y el dólar.
Triangulo perfecto de las monedas.

La primer característica es la escasez. El dólar, y en general las monedas locales de cada país, no tiene un límite, ya que pueden ser emitidas en cualquier momento. Sin embargo sabemos que el oro en la tierra es finito, y a su vez, sabemos que solo van a existir 21 millones de bitcoins.

Después tenemos la durabilidad. Más de una vez hemos recibido un billete cortado o con una cinta o una moneda oxidada, pero ni el oro ni Bitcoin se gastan o rompen con el paso del tiempo.

4. DIFERENCIAS ENTRE BITCOIN, ORO Y DOLAR

Si miramos el uso y adopción, el que tiene la ventaja actualmente es el dólar, ya que tiene varios años más de historia que el Bitcoin y a su vez es mas fácil de usar que el oro.

Respecto a la portabilidad, el oro se lleva la peor parte debido a su gran peso, mientras que el dólar tiene una posición neutral, ya que es fácil de llevar en bajas cantidades pero para transportar grandes volúmenes tiene sus complejidades adicionales. En cambio Bitcoin, tiene la ventaja de ser digital, por lo que independientemente del monto puede ser enviado a cualquier parte del planeta sin costos adicionales. Podemos llevarlo en un papel.

Si hablamos de divisibilidad, el oro es el más comprometido, ya que es poco práctico pagar en el supermercado 9,2 gramos de oro por una compra. El dólar y el Bitcoin tienen la facilidad de poder dividirse fácil.

4. DIFERENCIAS ENTRE BITCOIN, ORO Y DOLAR

Al hablar de Almacenamiento, el oro es el peor ubicado por su elevado peso y costo de almacenamiento, mientras que el dólar es neutral, ya que grandes cantidades de dólares tienen un costo de almacenamiento muy grande. Por su parte, Bitcoin tiene la ventaja de ser digital y no ocupar espacio físico.

Cuando analizamos la dificultad para la falsificación de la moneda, el dólar y el oro son neutros, ya que se pueden falsificar billetes y hay algunos lugares que venden otros metales como si fueran oro. En cambio, con bitcoins no es posible hacerlo porque su compleja tecnología criptográfica no lo permite.

- **¿Ordenadores quanticos podrán hackearlo? Si pero no solo al bitcoin sino a todo.**

4. DIFERENCIAS ENTRE BITCOIN, ORO Y DOLAR

Las tres funciones del dinero: Medio de intercambio, Unidad de Cuenta y Reserva de Valor:

- 1.- Medio de pago
- 2.- Unidad de cuenta
- 3.- Reserva de valor

No hay un banco central en Bitcoin ni en el oro físico.

El Bitcoin y el oro físico son primos cercanos con objetivos muy similares que se complementan muy bien para proteger nuestros ahorros a largo plazo en un mundo lleno de incertidumbres económicas y monetarias. Aunque me quedo con el Bitcoin antes que con el oro.

4. DIFE



1. DIFERENCIAS ENTRE BITCOIN, ORO Y DOLAR

CryptoCompare Index : BTC





VS



VS



Pellmellism.com i type stuff sometimes January 3 2014

	GOLD	BITCOIN	DOLLAR
Spendable	XX	✓✓✓ Hungry? Buy a Snickers - Good Luck 25¢ tip? \$500 Plane Ticket? \$200k Lambo? QR please	✓ Is that bill real - We need \$1's please - I cant break that, sorry
Anonymous	XX Did you bring the scale? Is it pure? Is it stolen?	✓✓✓ No name or address needed	✗ Cash? yes - Card? No
Transfer Delay	XXX Armored Trucks mostly obey speed limits - Forget transatlantic	✓✓✓ Near instant - Optional and trivial miner fee	XXX 3-7 day wire transfer - Check hold period - Heavy middle man fees
Transaction Fee	XXX and storage premium and conversion fee	✓✓✓ Suggested Miner fee - not necessary	XXX Thats the name of the game.
Non-Counterfeitable	XXX Pyrite? Spray Paint? Solid or plated?	✓✓✓ Public authenticity confirmation	XXX The pen test is a Ph test - try bleach
Theft Resistant	XXX Armored Truck - Armed Security - Expensive Heavy Safe	✓✓✓ With proper precautions theft becomes impossible	XXX Even big banks still get robbed - not to mention grandmas purse
Open Source	XXX When was the last audit on Fort Knox?	✓✓✓ 100%	XXX The Federal reserve isn't even Federal - it is a private corporation
Durability	XX Soft metal	✓✓✓ Binary	XXX Made out of paper
Inflation Proof	✓ Future space exploration problems are a ways off still	✓✓✓ 100% predetermined with a fixed supply	XXX Not even close
Irreversible Payments	✓ Possession is 99 percent of the law	✓✓✓ Impossible	XXX Merchants need more headaches
Decentralized	✓ Decentralized? Yes - Manipulated Market? Yes	✓✓✓ P2P	XXX Exactly the opposite
Divisibility	✓✓✓ Down to the atomic level	✓✓✓ 1 BTC = 10^8 satoshis = 100,000,000 satoshis	XXX Talk of removing the penny soon.
Scarcity	✓✓✓ Difficult to mine - Limited supply	✓✓✓ Fixed amount	XXX Can it print any faster? Then buy another printer!
Non-Monetary Usefulness	✓✓✓ Jewelry Electronics Dentistry Aerospace etc	✓✓✓ Proof of existence	XXX Is that a roll of quarters in your pocket or...
Shininess	✓✓✓ Extremely Shiny	XXX Not actually physical	XXX Filthy - Wear gloves or wash your hands

5. ¿Cómo usar Bitcoin o cualquier otra criptomoneda?

¿CÓMO USAR BITCOIN (CRIPTOMONEDA)? La criptomoneda bitcoin puede ser usada en cualquier tipo de transacción tanto comercial como financiera en el mundo real.

AMBITO REAL. En el ámbito comercial, bitcoin se puede usar para pagar compras en línea de una infinidad de productos, directamente en tiendas virtuales y comprar tarjetas de regalo (gift cards) para usar en tiendas como Amazon, iTunes, Starbucks, eBay y muchas más. También se pueden pagar compras en tiendas físicas que acepten la criptomoneda, tales como restaurantes, comercios, clínicas, supermercados, etcétera.



<https://coinmap.org/#/map/40.42894144/-3.68411064/16> www.localbitcoin.com

En el **AMBITO FINANCIERO**, el criptomoneda bitcoin se emplea para el ahorro, la inversión, el envío de remesas a familiares y amigos y realizar préstamos a individuos o empresas con quienes se haya acordado los términos y condiciones de tal operación.

5. ¿Cómo usar Bitcoin o cualquier otra criptomoneda?

REQUERIMIENTOS BÁSICOS. Para que cualquier persona o entidad pueda realizar las transacciones con Bitcoin debe tener una cartera digital Bitcoin, monedero (Bitcoin Wallet) y mantener saldo de bitcoins en ella.

Para abrir (crear) un monedero digital Bitcoin, el usuario debe saber que tipo de cartera quiere tener. Existen básicamente tres tipos de monederos:

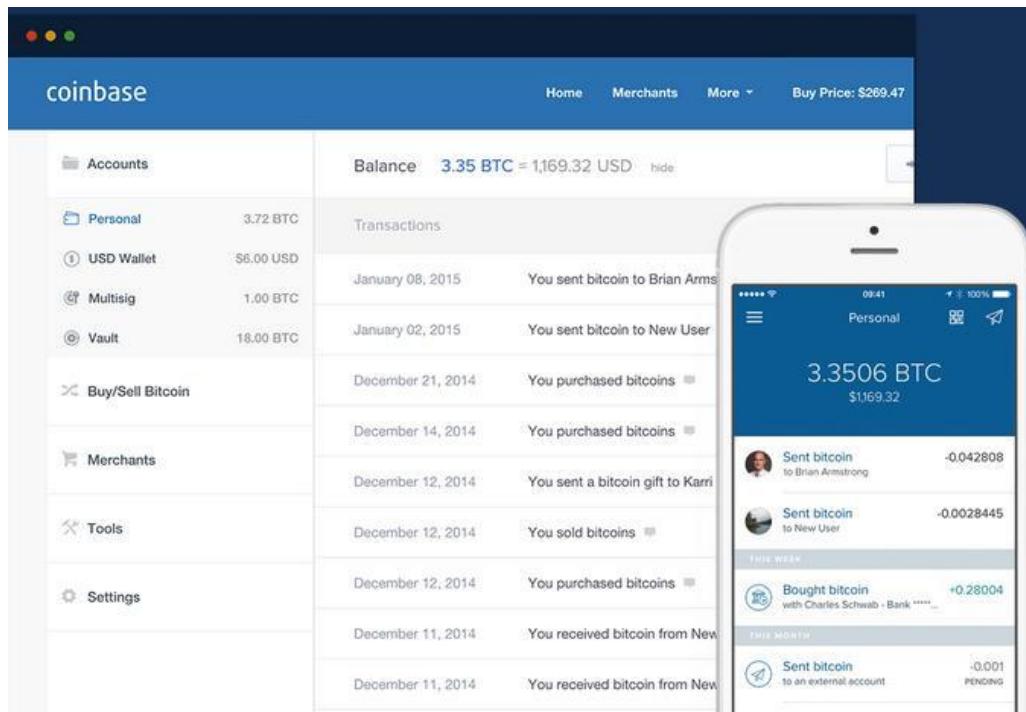
- Monederos hardware o monederos frios: como trezor.
- Aplicaciones independientes (apps) instaladas en computadoras o teléfonos móviles, de descarga gratuita, mycelium
- Cuentas online en alguna plataforma de monederos de criptomonedas de alguna empresa, los cuales pueden ser vistos como cuentas bancarias de criptomonedas.

Según el tipo de cartera tendremos unos beneficios u otros: las aplicaciones independientes otorgan anonimato y mayor seguridad pero, sin los cuidados necesarios, el usuario puede perder su clave privada o su respaldo y, con éstos, sus bitcoins.

Los monederos online eliminan el problema de las claves y respaldos, pero sacrifican el anonimato y agregan factores externos de riesgo: hacks a la plataforma, indisponibilidad de fondos, entre otros. Los monederos hardware: deterioro o perdida.

5. ¿Cómo usar Bitcoin o cualquier otra criptomonedas?

Al crearse la cartera digital se generan dos claves digitales, una clave pública, dirección bitcoin o número de cuenta del usuario, que permite que se reciban depósitos en la cartera, y una clave privada del usuario dueño de la cartera que permite transferir criptomonedas a otras carteras de otros usuarios para pagar o, en términos generales, concretar alguna transacción comercial o financiera que haya realizado.



5. ¿Cómo usar Bitcoin o cualquier otra criptomoneda?

¿CÓMO FUNCIONA LA TRANSACCIÓN?

- Si el usuario va a pagar una compra en línea, usualmente debe escoger la opción de pago con bitcoin, escanear el código QR o copiar la dirección bitcoin del vendedor en su monedero digital, verificar los datos (cantidad y clave pública), colocar su clave privada para aceptar la transacción y enviar. Dependiendo del servicio de pago que use el vendedor, éste liberará el producto o servicio adquirido instantáneamente o luego de 1 a 3 confirmaciones en la red Bitcoin, hasta un máximo de 6. Por ejemplo Bittrex te envía un email para confirmar el envío de BTC de tu monedero hacia afuera.
- Cuando se desea recibir bitcoins, el usuario deberá dar a la persona que envía las criptomonedas su clave pública o dirección bitcoin. Luego, la persona que envía deberá configurar la transacción en su cartera de bitcoins, esto es, colocar la cantidad enviar, la dirección bitcoin de la persona que recibe y aprobar la transacción mediante el uso de su clave privada. Al finalizar, la transacción se ejecutará y aparecerá reflejado el débito y crédito, en los respectivos lados de la operación, instantáneamente. Ejemplo Bittrex te añade los BTC a tu cartera luego de 2 confirmaciones, sino te lo pone en pending.

5. ¿Cómo usar Bitcoin o cualquier otra criptomonedada?

Importante: aunque el cambio se refleje instantáneamente en los balances de los monederos de cada usuario, la veracidad de las transacciones debe ser confirmada. La transacción será propagada por la red Bitcoin para ser confirmada por la red de mineros e incluida en un bloque de la cadena de bloques o block chain. Cada confirmación que la red otorgue a una transacción reduce en gran medida la probabilidad de fraude, agregándole así, legitimidad y confianza. Se recomienda esperar un cierto número de confirmaciones antes de usar los fondos: para transacciones pequeñas (1 BTC o menos), 3 confirmaciones; para transacciones grandes (más de 1 BTC), 6 confirmaciones.

Cuanta mas comisión paguemos a la hora de hacer una transacción mas rápido será todo, hacemos que la red confirme nuestra transaccion antes que otra, asignamos prioridad.

5. ¿Cómo usar Bitcoin o cualquier otra criptomonedada?

<https://blockchain.info/wallet/#/transactions>

Ejercicio obligatorio crear monedero en blockchain.info

July 14 @ 01:36 PM

Enviado

0.01717945 BTC

donation 

Para: 3Q2aKEGFTKDw3hghsBifXp39CZVMtZukxn
De: 1AokP9W85pRrH1TdvfyAVuMvPUpi3Jyie

Valor Enviado: \$11.35

Transaction Fee: 0.0004639 BTC

 Transacción completa ✓

May 15 @ 08:33 PM

Enviado

0.16247617 BTC

Add a description

Para: 1AgioizbbxHVcFeBKNpE6dAntnAjN1T7GU
De: 1AokP9W85pRrH1TdvfyAVuMvPUpi3Jyie

Valor Enviado: \$74.41

Transaction Fee: 0.0004 BTC

 Transacción completa ✓

<https://hollytransaction.com/images/infographics/why-are-transaction-fees-necessary-when-sending-bitcoin.png>

¿Qué son los Bitcoins? "On line"

- 45 -

Documentación recopilada por Mariano Hernando.

2016

5. ¿Cómo usar Bitcoin o c

Coinbase

AGO 10		Sent bitcoin a dirección bitcoin – hashflare script	-0,1506 BTC -79,72 € EUR
AGO 10		Sent bitcoin a dirección bitcoin – hashflare ethath	-0,2369 BTC -125,40 € EUR
AGO 10		Sent bitcoin a dirección bitcoin – hashflare sha256	-0,3410 BTC -180,51 € EUR
AGO 04		Bitcoin comprado using Visa debit *****7840	+0,18514277 BTC +100,00 € EUR
AGO 03		Bitcoin comprado using Visa debit *****7840	+0,18711172 BTC +94,00 € EUR
AGO 02		Bitcoin comprado using Visa debit *****7840	+0,07237087 BTC +40,00 € EUR
AGO 01		Bitcoin comprado using Visa debit *****7840	+0,03125559 BTC +18,00 € EUR
JUL 31		Bitcoin comprado using Visa debit *****7840	+0,09961046 BTC +59,00 € EUR

Cómo funciona una transacción con Bitcoin

Bob, un vendedor online, decide aceptar bitcoins como medio de pago
Alice, una compradora, quiere gastar sus bitcoins comprando algo a Bob.

MONEDEROS Y DIRECCIONES



Bob y Alice cuentan con monederos en sus ordenadores



Los monederos permiten el acceso a direcciones de Bitcoin



Una dirección es una cadena de letras y números.

Tipo:
IEH5ej MWeE
45ulrtJU4
LCWrfdPn

Bob crea una nueva dirección para que Alice le envíe el pago.

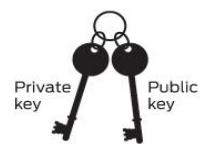
CREANDO UNA NUEVA DIRECCIÓN



Cada dirección tiene su propio balance de bitcoins



REALIZANDO UN PAGO



Public Key Cryptography 101

Cuando Bob crea una nueva dirección realmente está generado una clave de criptografía asimétrica, compuesta por una clave pública y otra privada. Cuando se incorpora una clave privada -solo tú conoces la clave- puede ser verificada con una clave pública, conocida por todos. La nueva dirección de Bitcoins de Bob representa una clave pública única, y la clave privada es la que está alojada en su monedero. La clave pública permite verificar que la firma con la clave privada es válida.



Alice comunica a su cliente Bitcoin la transferencia que quiere realizar a Bob.



Clave privada

El monedero de Alice cuenta con una clave para cada dirección. El cliente de Bitcoin de Alice demandará la clave para poder hacer la transacción.



Clave privada

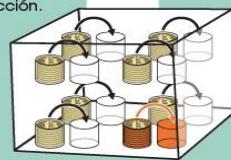
En este momento, cualquiera en la red puede verificar que la transacción que va a realizarse es veraz y pertenece a una cuenta legítima.

VERIFICANDO LA TRANSACCIÓN

Cary, Garth y Glenn son mineros de Bitcoin.



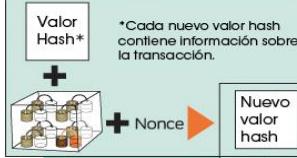
Sus ordenadores convierten la transacción pasados 10 minutos en un nuevo código de transacción.



Los ordenadores de los mineros están configurados para resolver funciones hash criptográficas.

TRANSACCIÓN VERIFICADA

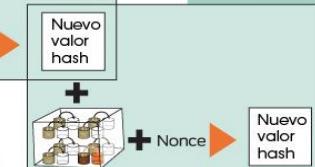
En poco tiempo, la transferencia de Alice a Bob quedará enterrada detrás de otras transacciones más recientes. Ahora ya no se puede deshacer la transacción por el propio mecanismo de seguridad de Bitcoin. Bob podrá devolver los bitcoin a Alice, empezando de nuevo el mismo mecanismo de pago seguro.



*Cada nuevo valor hash contiene información sobre la transacción.



Los ordenadores que minan calculan los valores hash basados en la combinación de los hash previos y el nonce.



The root of all evil ??? ➔ 0000 0000 0000 ...

La creación de los hashes es totalmente trivial, pero el sistema requiere que los nuevos valores hash tengan una forma particular y definida. Por ejemplo, debe empezar con ceros.

The root of all evil ➔ 6d0a1899 086a... (56 more characters)

The root of all evil ➔ 486c 6be4 6dde...

The root of all evil ➔ b8db 7ee9 8392...

Nonces

Para crear diferentes valores hash de una misma serie de datos, Bitcoin usa "nonces".

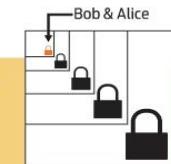
Un nonce es un número aleatorio incorporado a los datos antes del hash. Cambiando el nonce, los resultados son completamente distintos.



Los mineros no pueden predecir qué nonce produce qué valor hash.



Cada bloque minado incluye una transacción "coinbase" que paga 50 bitcoins al minero. En este caso, fue Gary, quién ahor cuenta con 50 bitcoins en un nuevo monedero.



5. ¿Cómo usar Bitcoin o cualquier otra criptomonedada?

IS BITCOIN ANONYMOUS?



Though lauded as a faceless way to send and receive money, Bitcoin is not an anonymous currency. Transactions are transparent, due to the open nature of the Blockchain ledger. Rather, Bitcoin is pseudonymous, as neither a wallet's owner, nor the reason for a transaction are apparent from blockchain data alone. Once a wallet's owner is identified however, they are easily linked to every transaction they have made.

What options does an individual have to keep their data private, and will true anonymity ever be possible with Bitcoin?

Mixing services mix your coins with other peoples' money in an attempt to obfuscate each coin's original source.	Reusing wallet addresses is not suggested, as it is harmful to both your own privacy, and the privacy of the people with whom you transact.	Be aware of who you share your personal information with online. In some countries, companies are required to store your data.	Some implementations such as CoinJoin, Stealth addresses, and Bip47 are designed to offer far greater privacy than Bitcoin does.	Future solutions and services for Bitcoin users seeking anonymity are likely to be developed in the years to come.

HolyTransaction

<https://holytransaction.com/page/why-are-bitcoin-transactions-irreversible>

<https://holytransaction.com/page/is-bitcoin-anonymous>

WHY ARE BITCOIN TRANSACTIONS IRREVERSIBLE?

Bitcoin allows two people to exchange an agreed upon sum via a process which is trustless and completely free of third party arbitration.

Since there is no intermediary involved in Bitcoin transactions, once a coin's ownership changes, the previous holder immediately loses the permissions necessary for moving or retrieving the coin.

For this reason, once bitcoin has been sent, the transaction can not be reversed unless the new owner agrees to return the coin to you.

As a bitcoin's ownership travels from one address to another, its record is updated within the Blockchain ledger.

HolyTransaction

5. ¿Cómo usar Bitcoin o cualquier otra criptomonedada?

¿Cómo de anónimo es hoy Bitcoin? Debemos de ser conscientes de que el Bitcoin es menos anónimo que el dinero en efectivo. Hay usuarios que han encontrado la manera de adquirir y usar Bitcoin de forma anónima, pero la naturaleza abierta de la contabilidad de las transacciones dejan abierta la posibilidad de que las identidades y actividades que antes se consideraban perfectamente seguras puedan ser revelados en algún momento.

¿Y en el futuro? Según vaya en aumento la adopción de Bitcoin, se irá creando una carrera entre los anonimizadores y los deanonymizadores: por un lado, se desarrollarán planes de minería de datos cada vez más sofisticados, posiblemente combinando el análisis gráfico de transacción con el descubrimiento de direcciones IP, para rastrear el movimiento de fondos de la cadena de bloques entre individuos y entre fronteras. Por otro lado se diseñarán nuevas estrategias para ocultar mejor la identidad individual y la actividad.

Hay muchas incógnitas. ¿Se modificará el código Bitcoin para proteger aún más el anonimato o para facilitar la regulación? ¿Alcanzará el análisis gráfico de transacción tal grado de sofisticación en el que la mayoría de las actividades del usuario se puedan rastrear fácilmente? ¿Surgirá una moneda alternativa o una cadena lateral que incline la balanza a favor o en contra del anonimato?

4. ¿Cómo usar Bitcoin o cualquier otra criptomoneda?

¿Qué es la web profunda o el Deep web?

Se conoce como web profunda (Deep web, en inglés) a todo el contenido de Internet que no está indexado por los motores de búsqueda de la red. Puede usarse el término Internet o web invisible también para referirse a ella.

La web profunda está pues compuesta de páginas o repositorios de información, generalmente sitios generados dinámicamente, cuyo contenido no puede ser revisado por los motores de búsqueda, y por lo tanto, no está incluido en sus resultados de búsqueda.

Se utilizan monedas lo mas anónimas posibles para hacer transacciones en la deep web: monero. Es necesario que todo tenga su criptomoneda incluido el crimen. <https://getmonero.org/home> y <https://www.dash.org/es/>

<http://criptonoticias.com/adopcion/mercados-deep-web-impulsan-precio-criptomoneda-monero/>

<http://www.diariobitcoin.com/index.php/2016/08/25/los-traficantes-de-la-deep-web-esperan-que-monero-sea-mas-anonima-que-bitcoin/>

6. ¿Cómo obtener Bitcoins?

8 formas de obtener bitcoins:

- Ganar Bitcoins aceptándolos como método de pago
- Ganar Bitcoins gratis completando pasos en páginas de internet
- Ganar Bitcoins como pagos de intereses, lending en poloniex
- Ganar Bitcoins minando.
- Ganar Bitcoins recibiendo donativos.
- Ganar Bitcoins haciendo trading
- Gana Bitcoins como ingreso regular por ejemplo cobrando nominas como en bitso Mexico.
- Gana Bitcoins apostando con el juego – (no es algo para todos)

Seguro que se nos ocurren mas formas de ganar bitcoins pero al menos estas.

6. ¿Cómo obtener Bitcoins? Faucet

¿Que es un faucet? Faucet es una palabra inglesa que significa “grifo”. En estas páginas se dan bitcoin de forma gratuita.

¿Por qué regalan bitcoin los faucet? Los faucet son páginas que regalan bitcoin, como modo de promocionar el uso de esta moneda. Cuanta más gente tenga bitcoins, más popular será y más fuerza tomará como medio de pago.

¿Cómo es posible?, ¿Regalan dinero? Sí. Regalan dinero, regalan bitcoins. Pero solamente es para que la gente nueva tenga sus primeros bitcoins y se anime a usar esta nueva moneda llamada bitcoin como medio de pago. En realidad regalan poco dinero, y, además, las páginas de faucets tienen publicidad, con lo cual con los ingresos de la publicidad mantienen vivo el faucet. <http://www.blockchainaliens.com/top-10-free-bitcoin-faucets/>

7. ¿CÓMO COMPRAR Y VENDER BITCOINS?

Actualmente hay cuatro formas muy bien definidas y establecidas para comprar y vender bitcoins y criptomonedas, que se incrementarán en un futuro cercano en la medida que la adopción de bitcoin se popularice aún más, tanto por la incorporación de nuevos usuarios y empresas que lo acepten, como por el desarrollo de nuevas aplicaciones basadas en esta tecnología.

Las formas actuales para comprar y vender bitcoin son:

1. Casas de cambio. Kraken, poloniex, bittrex, coinbase
2. *Entre personas (localbitcoin)*
3. *Cajeros automáticos (ATM)*
4. *Tiendas físicas o kioscos (Bitso: osso / seven eleven)*

7. ¿CÓMO COMPRAR Y VENDER BITCOINS?

CASAS DE CAMBIO (EXCHANGE)

La manera de comprar y vender bitcoins más usada actualmente es a través de casas de cambio, empresas online especializadas en la compraventa de criptomonedas. En éstas se pueden adquirir varias de las criptomonedas más importantes (BTC, ETH, XMR, LTC, entre otras) a tipos de cambio que fija el mercado. La compraventa de bitcoin en éstas se puede hacer con o por otras criptomonedas o con dinero fiat (USD, EUR, JPY, entre otras).

Para comprar y vender bitcoins a través de casas de cambio, el usuario deberá registrarse en el sitio web de la casa de su preferencia e ingresar los datos que la plataforma requiera para comenzar a operar. Estos datos pueden ir desde nombre completo, email y dirección de residencia, hasta número telefónico, pasaporte y estados de cuenta bancarios. **F2A. Ya se pierde claramente el anonimato, estas igual de controlado que en banco**

Las casas de cambio cobran una comisión por transacción de compra o venta y otra por transferencia de fondos a la cuenta bancaria del cliente, en caso de venta de bitcoin por dinero fiat. Como las comisiones varían entre casas de cambio, el usuario debe realizar su estudio para minimizar estos costos, para un mismo nivel de seguridad de la casa de cambio. En 2016 las comisiones que se pagan son altas.

7. ¿CÓMO COMPRAR Y VENDER BITCOINS?

CASAS DE CAMBIO (EXCHANGE) que vamos a ver ahora:

- KRAKEN
- COINBASE
- POLONIEX
- BITTREX



<https://www.buybitcoinworldwide.com/es/>

7. ¿CÓMO COMPRAR Y VENDER BITCOINS?

Las criptomonedas tienen transacciones en todo momento, 24 horas al día x 365 días al año, bisiestos incluidos.

NO EXISTE CALENDARIO TARGET

Preponderancia de china tanto en minería como en trading

7. ¿CÓMO COMPRAR Y VENDER BITCOINS?

PERSONAS NATURALES

Esta segunda forma de compraventa es posible gracias a la descentralización que proporciona la red, la cual permite al interesado comprar y vender bitcoins directamente a personas cercanas, o simplemente conocidos de internet con los que haya decidido concretar algún acuerdo de intercambio monetario. Para la compraventa de bitcoins directamente entre personas, que se conozcan o no, los interesados únicamente deberán poseer sus respectivos monederos bitcoin y cuentas bancarias, en caso de intercambio por dinero FIAT. El retraso de la transferencia bancaria para la disponibilidad del dinero fiduciario, que puede ser de días, y la necesidad de varias confirmaciones de la transacción en la red, para asegurar la disponibilidad de la criptomonedra en el monedero Bitcoin, que toma varios minutos, originan el riesgo de fraude.

<https://localbitcoins.com/>

https://localbitcoins.com/es/vender_bitcoins

https://localbitcoins.com/es/comprar_bitcoins

<https://localbitcoins.com/es/comprar-bitcoins-online/usd/paypal/>

7. ¿CÓMO COMPRAR Y VENDER BITCOINS?

El fraude ocurre porque una de las partes incumple su compromiso, ya sea porque no envía la transferencia bancaria o la anula luego de notificarla a su contraparte, o porque incurre en un doble gasto de la criptomoneda objeto del intercambio. Lo más adecuado para reducir este riesgo es que la operación de compraventa la realicen las partes lo más simultáneamente posible y la transferencia de fondos se realice entre cuentas del mismo banco, para reducir el tiempo de disponibilidad de fondos a minutos o menos. De ahí que en este tipo de intercambio la confianza juega un papel fundamental. Por ello, se debe ser muy cuidadoso a la hora de comprar o vender bitcoins entre personas directamente.

Algunas maneras de mitigar este riesgo son:

- Acordar una reunión en persona, en caso de que sea posible.
- Utilizar un intermediario, ya sea una persona de confianza entre ambos interesados o un servicio de garantías, comúnmente conocido como “escrow”. Los intermediarios pueden cobrar una comisión por el arbitraje en el intercambio de dinero.

7. ¿CÓMO COMPRAR Y VENDER BITCOINS?

The screenshot shows the LocalBitcoins.com homepage. At the top, there's a banner with the text "Buy and sell bitcoins near you", "Instant. Secure. Private.", and "Trade bitcoins in 13345 cities and 248 countries including Spain.". Below the banner is a green "Sign up free" button. Underneath, there are two tabs: "QUICK BUY" (selected) and "QUICK SELL". A search bar includes fields for "Amount", "EUR", "Spain", "All online offers", and a "Search" button. Below this, a section titled "Buy bitcoins online in Spain" lists five sellers:

Seller	Payment method	Price / BTC	Limits	Action
gugamuga (100+; 100%)	SEPA (EU) bank transfer: EEUHEE2X	554.49 EUR	100 - 277 EUR	Buy
kaene (100+; 100%)	Hal-cash	559.13 EUR	50 - 600 EUR	Buy
MSTC (500+; 100%)	Hal-cash	560.00 EUR	50 - 560 EUR	Buy
doche (30+; 100%)	National bank transfer: Spain	560.07 EUR	250 - 1829 EUR	Buy
gaoqep (25; 100%)	Hal-cash	561.79 EUR	50 - 230 EUR	Buy

7. ¿CÓMO COMPRAR Y VENDER BITCOINS?

CAJEROS AUTOMÁTICOS

A lo largo de estos últimos años han habido empresas en varios países han instalados cajeros automáticos o ATMs para la compraventa de bitcoins, y otras criptomonedas. Dependiendo de las capacidades del cajero, se podrán comprar criptomonedas por dinero en efectivo (lo más común) o también vender bitcoins por éste.

Para utilizar un cajero de bitcoins, el usuario deberá poseer una cartera de criptomonedas, habitualmente en el móvil. Si la operación es una compra de bitcoins, el usuario deberá seleccionar dicha operación en el ATM, presentar el código QR de su cartera al lector del cajero, introducir el dinero que quiere usar en la compra, verificar la cantidad de bitcoins que recibirá a cambio y aceptar la compra.

Si lo que desea el usuario es vender bitcoins, deberá seleccionar esta operación en el ATM, introducir el monto en moneda fiduciaria que quiere obtener y aceptar la venta. Esta operación generará una cartera de papel con un código QR a la cual el usuario deberá enviar las criptomonedas (dentro del tiempo establecido para mantener la misma tasa de cambio). Una vez que se hayan dado dos o más confirmaciones en la red, el usuario deberá seleccionar la opción de “redimir” en el cajero, presentar el código QR de la cartera de papel al lector del cajero o introducir algún código que aparezca en el papel dispuesto para retirar el dinero (según sea el caso), confirmar el retiro y tomar su dinero en efectivo.

Algunos cajeros de criptomonedas piden documentos de identificación para realizar transacciones. Por su parte, los operadores de los cajeros automáticos de bitcoins cobran un porcentaje fijo sobre el monto de la transacción realizada (comúnmente entre 0% y 7,5%).

7. ¿CÓMO COMPRAR Y VENDER BITCOINS?

CAJEROS AUTOMÁTICOS

Ejemplos de instalación de cajeros automáticos:

<http://criptonoticias.com/cajeros-automaticos/atms-bitcoin-exchange-cajero-automatico-asturias/>
<http://criptonoticias.com/cajeros-automaticos/atms-bitcoin-exchange-sl-instala-nuevos-cajeros-bitcoin-espana/>
<http://criptonoticias.com/cajeros-automaticos/cryptoatm-construye-tu-propio-cajero-automatico-bitcoina/>
<http://criptonoticias.com/cajeros-automaticos/islas-baleares-primer-cajero-automatico-bitcoin/>
<http://criptonoticias.com/cajeros-automaticos/centro-comercial-madrid-recibe-primer-cajero-bitcoins/>
<http://criptonoticias.com/cajeros-automaticos/filial-deloitte-instala-nuevo-cajero-bitcoin-canada/>
<http://criptonoticias.com/colecciones/cajeros-automaticos-bitcoin-latinoamerica-espana/>
<http://criptonoticias.com/?s=cajeros>

<https://www.youtube.com/watch?v=nGfbaLKCvPM>

Video del primer cajero Bitcoin se instala en Madrid. Publicado el 31 oct. 2014 . Antonio García Navarro, presidente de Bitcoin Spain nos muestra el funcionamiento del primer cajero automático para comprar y vender Bitcoin, del fabricante Robocoin, que se ha instalado en Madrid en el hotel One Shot Recoletos, situado en la calle Salustiano Olózaga 4.

7. ¿CÓMO COMPRAR Y VENDER BITCOINS?



7. ¿CÓMO COMPRAR Y VENDER BITCOINS?

TIENDAS FÍSICAS O KIOSCOS

Existen miles de tiendas físicas o kioscos alrededor del mundo que permiten comprar bitcoins con dinero en efectivo o con tarjetas de débito. Estos kioscos requieren muchas veces que el usuario rellene un formulario con datos personales y de la compra, antes de enviar al usuario los bitcoins o entregar una cartera de papel, voucher o tarjeta de regalo. Al igual que los operadores de cajeros automáticos, los kioscos cobran un porcentaje fijo sobre el monto de la transacción realizada (comúnmente entre 5% y 16%), son los mas caros pero a la vez es lo mas sencillo.

Ejemplo: Bitso.com Fácil y accesible. Fondea tu cuenta en tiendas de conveniencia como Oxxo y 7-Eleven. Más de 135,000 locaciones en México.

<https://help.bitso.com/support/solutions/folders/1000211010>

<https://blog.bitso.com/latest> (BITSO es todo)

<https://blog.bitso.com/zmart-y-bitso-llevan-bitcoin-a-tu-tiendita-47e367e99eef?source=latest>

<http://criptonoticias.com/aplicaciones/zmart-group-permitira-compra-bitcoins-20-000-tiendas-alimentos-mexico/>

<http://criptonoticias.com/adopcion/coinapult-300-localidades-colombia-para-comprar-bitcoins/>

7. ¿CÓMO COMPRAR Y VENDER BITCOINS?

EJEMPLO PRACTICO Tutoriales: Fondear tu Cuenta DE BITSO

Fondear tu Cuenta Introducción.

Tutorial: Recibir bitcoins en tu cuenta de Bitso

Tutorial: Fondear cuenta cuenta por medio de SPEI

Tutorial: Fondear en Efectivo por medio de ComproPago [Oxxo, 7Eleven, Extra, Walmart y más]

Tutorial: Canjear Cupón de Bitso

Tutorial: Fondear tu Cuenta por Medio de Transferencia Internacional

Tutorial: Fondear tu cuenta con Pademobile

7. ¿CÓMO COMPRAR Y VENDER

FINAL SUMMARY

BTC ATM

BTMs have begun popping up everywhere. Search for the nearest one to you online, and take cash and at least one form of identification with you. BTMs are fast, once an account is set up. They can trade in large quantities, and can buy back when you're ready to sell. BTMs document your personal information, in compliance with government standards. Coins are marked up significantly. Call before visiting, because they are often out of service. COST: 6% fee or higher TIME: 10-30 Minutes (not including travel time)

LOCAL MEETUP

Service such as LocalBitcoins and Mycelium trader allow you to find people in your area who are buying and selling coins. Meet new people with common interests, trade quickly in person using a phone or computer. Can often be inexpensive, depending on the seller. Due to possible stranger danger, insist on meeting in a public place, and take a friend with you. COST: 3 - 20% markup TIME: 10 Minutes (not including travel time)

WEB MERCHANTS

Some online services allow you to purchase Bitcoin by utilizing online merchants such as PayPal or a Debit Card. Buyers are protected by PayPal in case a seller tries to scam you by never sending coins. Legitimate transactions are fast and easy. PayPal and Debit card sellers are almost impossible to find, because it is too easy for buyers to process a chargeback on purchased coins. You'll need to build a rapport with the seller before they'll be willing to trade. COST: 10%+ markup TIME: 10 - 30 minutes

BANK WIRE

Recently, wallet providers such as Circle have begun linking customers Bank accounts to their profiles, allowing trade between them. Extremely fast, simple, and reliable. Personal information is required in compliance with government standards. Limits may be placed on buy, sell, and transfer amounts, and assets may occasionally be frozen or inaccessible. Accounts take 1-3 days to link at first use. COST: 1 - 3% fee TIME: Instant, once approved.

WHAT ARE THE FASTEST WAYS TO TRADE CASH FOR BITCOIN?

	BTC ATM	LOCAL MEETUP	WEB MERCHANTS	BANK WIRE
OPTIONS				
PROCESS	BTMs have begun popping up everywhere. Search for the nearest one to you online, and take cash and at least one form of identification with you.	Service such as LocalBitcoins and Mycelium trader allow you to find people in your area who are buying and selling coins.	Some online services allow you to purchase Bitcoin by utilizing online merchants such as PayPal or a Debit Card.	Recently, wallet providers such as Circle have begun linking customers Bank accounts to their profiles, allowing trade between them.
PROS	BTMs are fast, once an account is set up. They can trade in large quantities, and can buy back when you're ready to sell.	Meet new people with common interests, trade quickly in person using a phone or computer. Can often be inexpensive, depending on the seller.	Buyers are protected by PayPal in case a seller tries to scam you by never sending coins. Legitimate transactions are fast and easy.	Extremely fast, simple, and reliable.
CONS	BTMs document your personal information, in compliance with government standards. Coins are marked up significantly Call before visiting, because they are often out of service.	Due to possible stranger danger, insist on meeting in a public place, and take a friend with you.	PayPal and Debit card sellers are almost impossible to find, because it is too easy for buyers to process a chargeback on purchased coins. You'll need to build a rapport with the seller before they'll be willing to trade.	Personal information is required in compliance with government standards. Limits may be placed on buy, sell, and transfer amounts, and assets may occasionally be frozen or inaccessible. Accounts take 1-3 days to link at first use.
COST & TIME	COST: 6% fee or higher TIME: 10-30 Minutes (not including travel time)	COST: 3 - 20% markup TIME: 10 Minutes (not including travel time)	COST: 10%+ markup TIME: 10 - 30 minutes	COST: 1 - 3% fee TIME: Instant, once approved

8. ¿Cómo aceptar pagos en Bitcoin?

CÓMO ACEPTAR PAGOS EN BITCOINS?

Para recibir pagos en bitcoins se necesita poseer un monedero o billetera digital. Con este monedero se genera una llave pública, también conocida como dirección bitcoin, que puede estar asociada a un código QR, tal como se muestra ABAJO:



Código QR BTC

Dirección bitcoin: [1AokP9W85pRrH1TdvvfyAVuMvPUpi3Jyie](https://www.blockchain.info/address/1AokP9W85pRrH1TdvvfyAVuMvPUpi3Jyie)

Blockchain.info

Tarea: daros de alta en
blockchain.info

Enviadme vuestra dirección de
Bitcoin y os haré una donación de
bitcoins, algunos satoshis.

8. ¿Cómo aceptar pagos en Bitcoin?

El vendedor deberá dar a la persona que desea pagar con bitcoins la llave pública o el código QR, así como también la cantidad. Luego, la persona que paga deberá copiar la dirección en su cartera o escanear el código QR con la cámara de su móvil, introducir la cantidad a pagar y enviar los bitcoins.

En caso de no querer quedarse con los bitcoins, el comerciante deberá encargarse posteriormente de cambiar sus bitcoins por la divisa del país que desee a través de alguna casa de cambio & exchange o de una persona interesada.

También existe la posibilidad de facilitar el proceso de intercambio de bitcoins mediante el uso de procesadores de pago. Los procesadores de pago integran las carteras bitcoin y las casas de cambio, lo que hace posible el intercambio instantáneo de los bitcoins recibidos a cualquier divisa que la plataforma soporte. Además, también emiten facturas de la venta realizada. Un ejemplo interesante: https://bitso.com/merchant_info

8. ¿Cómo aceptar pagos en Bitcoin? Elegir un monedero Bitcoin

¿CÓMO ELEGIR UN MONEDERO BITCOIN?

Los monederos, carteras o Bitcoin wallets, almacenan las claves privadas que se necesitan para acceder a los bitcoins registrados en una dirección o clave pública para poder gastarlos. Los principales tipos de monederos disponibles en el mercado se pueden dividir en dos categorías, según sean aplicaciones independientes (apps) instaladas en dispositivos personales o, cuentas online abiertas en plataformas de empresas que prestan tal servicio.

Para la categoría de aplicaciones independientes hay tres tipos de monedero según el dispositivo que se use: monederos para pc, para móviles y monederos hardware. La seguridad de los bitcoins que se posean y cuyas claves de acceso se guarden en estos dispositivos dependerá únicamente del usuario, quién deberá realizar respaldo de la cartera y almacenarlo en un lugar seguro. Para ello, deberá crear las contraseñas de respaldo y de encriptación del monedero.

8. ¿Cómo aceptar pagos en Bitcoin? Elegir un monedero Bitcoin

A nivel de seguridad se pueden activar 2 contraseñas: la primera contraseña abre la billetera en cualquier equipo que pueda correr la aplicación; y la segunda permite mover los bitcoins que posea en la billetera. Ambas contraseñas deben ser fuertes, para evitar que alguien las descifre, y anotarse en varios lugares, para evitar olvidarlas o perderlas. Muy parecido a un banco: clave de acceso a la cuenta y clave de transferencia.

Si se utilizan carteras online, la seguridad dependerá del usuario y de la empresa que proporcione el servicio. El usuario deberá encargarse de colocar una contraseña fuerte y activar todas las medidas de seguridad que el sitio web provea: verificación de teléfono, autenticación de dos factores, preguntas secretas, entre otras. La empresa se encargará de la protección de la plataforma contra ataques y, en algunos casos, del aseguramiento de los bitcoins ante pérdidas. Ojo: el hackeo se suele dar en estas plataformas.

8. ¿Cómo aceptar pagos en Bitcoin? Elegir un monedero Bitcoin

CARACTERÍSTICAS BASICAS DE UN MONEDERO DE CRIPTOMONEDAS

Control sobre el dinero: las carteras de criptomonedas pueden permitir el manejo individual (solo el usuario posee las llaves privadas), el manejo conjunto (el dueño y la empresa poseen llaves privadas), o el manejo por parte de un tercero (la empresa posee las llaves privadas) del dinero almacenado en ellas.

Dependiendo del control sobre el manejo del dinero que se escoja, aumenta o disminuye la responsabilidad y control del usuario y la seguridad de los fondos en la cartera.

- Validación
- Transparencia
- Entorno
- Privacidad

<http://www.diariobitcoin.com/index.php/2016/06/15/los-5-mejores-monederos-bitcoin-para-usar-en-el-2016/>
<http://www.diariobitcoin.com/index.php/2016/01/15/como-escoger-el-mejor-monedero-bitcoin/>

8. ¿Cómo aceptar pagos en Bitcoin? Elegir un monedero Bitcoin

Validación: los monederos de criptomonedas pueden utilizar para validar las transacciones realizadas: validación completa (nodo completo, descarga en su totalidad la cadena de bloques), validación simplificada (nodo simple, solo descarga los hash del bloque), o validación centralizada (nodo completo de un tercero). Basado en el tipo de validación que utilice el monedero, se deberá confiar o no en que un tercero realice la correcta validación de las transacciones realizadas.

Transparencia: los monederos de criptomonedas pueden ser totalmente transparentes (el código de la aplicación puede ser auditado y verificado por el usuario), transparentes (el código puede ser auditado, pero no puede ser verificado por el usuario), o nada transparentes (el código de la aplicación es cerrado y la aplicación se corre en remoto). Dependiendo del grado de transparencia, el usuario deberá confiar más o menos en que el desarrollador de la aplicación no añadió códigos secretos o maliciosos que puedan hacer que pierda sus fondos o sean hurtados.

8. ¿Cómo aceptar pagos en Bitcoin? Elegir un monedero Bitcoin

Entorno: las carteras de criptomonedas pueden ser instaladas en entornos vulnerables (propensos a virus) con o sin autenticación de dos pasos, entornos seguros (como teléfonos móviles en los que las aplicaciones están aisladas), y entornos muy seguros (como carteras físicas de criptomonedas, gadgets). Dado el tipo de entorno usado, el usuario deberá activar mecanismos como la autenticación de dos pasos y colocar contraseñas complejas a sus carteras y dispositivos para evitar la pérdida o robo de fondos.

Privacidad: las carteras de criptomonedas pueden revelar o no información de sus usuarios a los nodos de la red (como por ejemplo la dirección IP), reusar o no las direcciones de las carteras con cada pago, y permitir o no el uso del navegador anónimo Thor para prevenir que otras personas o empresas puedan asociar las transacciones con la dirección IP del usuario. Dependiendo del tipo de privacidad que la cartera proporcione, el usuario deberá estar más o menos atento de la información que revela a la red.

8. ¿Cómo aceptar pagos en Bitcoin? Elegir un monedero Bitcoin

MONEDEROS PARA COMPUTADORAS PERSONALES



BITCOIN CORE



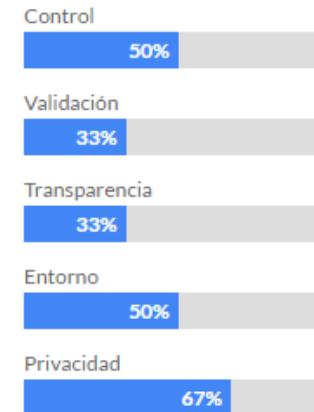
ELECTRUM



COPAY



BITGO



Con información de: bitcoin.org

<http://www.diariobitcoin.com/index.php/2016/01/15/como-escoger-el-mejor-monedero-bitcoin/>

8. ¿Cómo aceptar pagos en Bitcoin? Elegir un monedero Bitcoin

MONEDEROS PARA DISPOSITIVOS MÓVILES



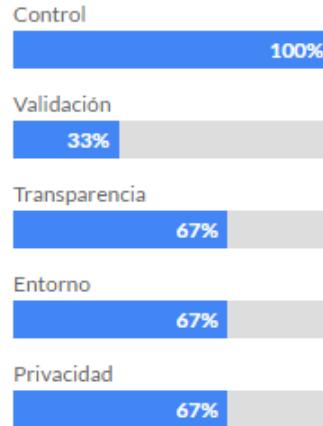
BITCOIN WALLET



MYCELIUM



COPAY



BREADWALLET



Con información de: bitcoin.org

8. ¿Cómo aceptar pagos en Bitcoin? Elegir un monedero Bitcoin

MONEDEROS FÍSICOS DE CRIPTOMONEDAS

<http://criptonoticias.com/colecciones/las-4-mejores-carteras-frías-de-bitcoin>



Carteras frías

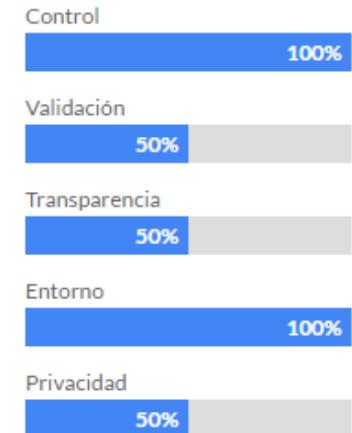
TREZOR



LEDGER NANO



KEEPKEY



Con información de: bitcoin.org

8. ¿Cómo aceptar pagos en Bitcoin? Elegir un monedero Bitcoin

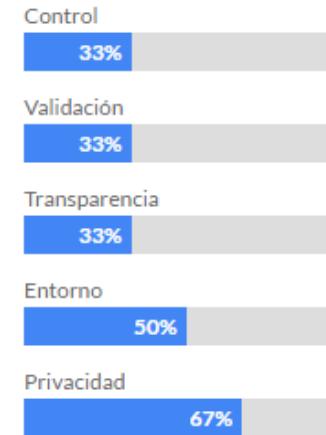
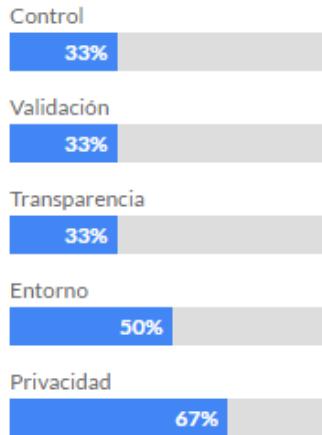
MONEDEROS EN LÍNEA EN PLATAFORMAS DE EMPRESAS



COINBASE

CIRCLE

XAPO



Con información de: bitcoin.org

| ¿Qué son los Bitcoins? "On line"

Documentación recopilada por Mariano Hernando.

8. ¿Cómo aceptar pagos en Bitcoin? ¿Qué es una billetera multifirma?

Firma-múltiple para proteger contra robo

Bitcoin incluye una característica multi-firma que permite a una transacción pedir la firma de más de una clave privada.

Multi-firma puede, por ejemplo, permitir a una organización dar acceso a la tesorería a sus miembros y permitir una extracción de dinero solo si 3 de los 5 miembros firman la transacción.

También permite a los monederos online compartir una dirección multi-firma con sus usuarios, de manera que un ladrón tenga que comprometer su ordenador y los servidores del monedero online para conseguir robar tus fondos.

Bitgo. <https://www.bitgo.com/>

8. ¿Cómo aceptar pagos en Bitcoin? ¿Qué es una billetera multifirma?

WHAT IS MULTISIG and why does it matter?

MultiSig transactions, short for multi-signature, give several users access to a single wallet. Cryptocurrency wallets have a public key, which is shared, and a private key, which is kept secret. Transactions must be signed with a user's private key in order to verify ownership, and validate a transaction.

MULTIPLE KEYS	M of N TRANSACTIONS	ADVANCED SECURITY
		
Multi-sig wallets have a public key with more than one private key.	Requires multiple parties to be in agreement to complete a transaction.	Provides extra security, making coins safer from theft.

 Multisig was first introduced in 2012, but did not become wide-spread until 2014.

 A multisig wallet may only require a certain number of its multiple users to validate a transaction.

 In 2014, less than 0.02% of BTC transactions were secured by multisig. That number is now 10%.

 Public addresses begin with the number 1. Multisig addresses begin with the number 3.



8. ¿Cómo aceptar pagos en Bitcoin? Formas de almacenar.

En un top 3 de formas mas seguras de almacenar los bitcoins tendriamos:

- 1 - Multifirma
- 2 - Trezor (monedero frio)
- 3 - PaperWallets (clave privada en papel)

Consejos de seguridad:

<https://bitcoin.org/es/asegure-su-monedero>

8. ¿Cómo aceptar pagos en Bitcoin? Formas de almacenar.

Las mal llamadas carterasPapel o PaperWallets, ni son carteras, ni tienen porqué ser de papel. Estas simplemente contienen la clave Privada de una dirección Bitcoin apuntada en un soporte físico. Propiamente debería llamarse dirección, porque de la clave privada se genera, como ya sabemos, las claves pública y privada de una dirección Bitcoin.

Grabar la clave privada en mármol, papel, acero, oro,...

Es por eso que se utiliza como soporte el papel o una tarjeta de plástico y, principalmente, el código QR. La dirección Papel más simple es solo la clave privada apuntada en un Papel. Nada más. Si se quiere también se puede añadir la clave pública. Normalmente está en formato QR, pero puede ser con todos los caracteres (números y letras). También podemos apuntar la clave privada en un procesador de texto y después lo sacamos en nuestra impresora y ya tenemos nuestra dirección Papel casera. O directamente en bolígrafo.

8. ¿Cómo aceptar pagos en Bitcoin? SEGURIDAD

EL BITCOIN ES SEGURO.

EL BITCOIN NO SE PUEDE ROBAR

SI TE ROBAN LO QUE TE ROBAN ES LA CLAVE PRIVADA Y POR ENDE TE PUEDEN TRANSFERIR LOS BITCOIN.

ES COMO SI TE ROBARAN LA CARTERA DEL BOLSILLO. TE QUITAN EL DINERO QUE ESTA DENTRO. SE ROBAN LOS MONEDEROS NO SE ROBAN LOS BITCOIN.

9. ¿QUÉ ES LA MINERÍA DE BITCOINS (CRIPTOMONEDAS)?

¿QUÉ ES LA MINERÍA DE BITCOINS (CRIPTOMONEDAS)?

En el proceso de consenso descentralizado que se produce en la red p2p con el objeto de validar las transacciones de los usuarios y evitar que las de doble gasto se incluyan en la cadena de bloques, los nodos de la red son recompensados con bloques de monedas digitales. La minería se puede ver como como un pago al nodo a cambio del servicio de crear un bloque en la cadena de consenso.

Esta compensación es un incentivo para que los nodos de la red p2p se comporten de manera honesta. Siendo la conducta de los nodos honestos extender siempre la cadena de bloques valida más larga, donde se supone están las transacciones validadas, no las de doble gasto. La protección contra el doble gasto es puramente el consenso de la red. Es el consenso el que determina cual transacción finaliza en la cadena de consenso valida más larga.

9. ¿QUÉ ES LA MINERÍA DE BITCOINS (CRIPTOMONEDAS)?

MINERÍA BITCOIN

De acuerdo a las reglas de Bitcoin, el nodo que crea un bloque puede incluir una transacción especial en ese bloque: una transacción de creación de monedas (coinbase). Además, el nodo también puede escoger la dirección de esta transacción, la cual, por supuesto, será la propia. Para crear un bloque, el nodo que propone ese bloque está obligado a conseguir un número arbitrario único o nonce que resuelve exitosamente un acertijo hash (hash puzzle), la criptografía.

El acertijo hash es un problema matemático que busca que el hash del bloque a crear se encuentre dentro de un espacio objetivo (target), que define la dificultad de minado y que depende del procesamiento total de la red. Para resolver este acertijo es necesario conseguir un número arbitrario único o nonce que al concatenarlo con el puntero hash del bloque previo y las transacciones que el nodo propone que el bloque contenga y aplicarle la función hash, hace que se cumpla la condición objetivo.

9. ¿QUÉ ES LA MINERÍA DE BITCOINS (CRIPTOMONEDAS)?

El espacio objetivo es ajustable para permitir que la dificultad del acertijo pueda ser cambiada en el tiempo a medida que nuevos usuarios entran a la red o antiguos usuarios la dejan, modificando la cantidad procesamiento total de la red. Esto permite que el acertijo sea lo suficientemente difícil para que ataques a la cadena de bloques sean costosos, pero las soluciones del acertijo pueden ser aún encontradas a una tasa casi fija (en el caso de Bitcoin, alrededor de diez minutos). La dificultad en general sube y la recompensa baja con el tiempo, cada 4 años halving y la recompensa baja a la mitad, ultimo halving julio de 2016 pasamos de 25 BTC por bloque a 12.5 BTC.

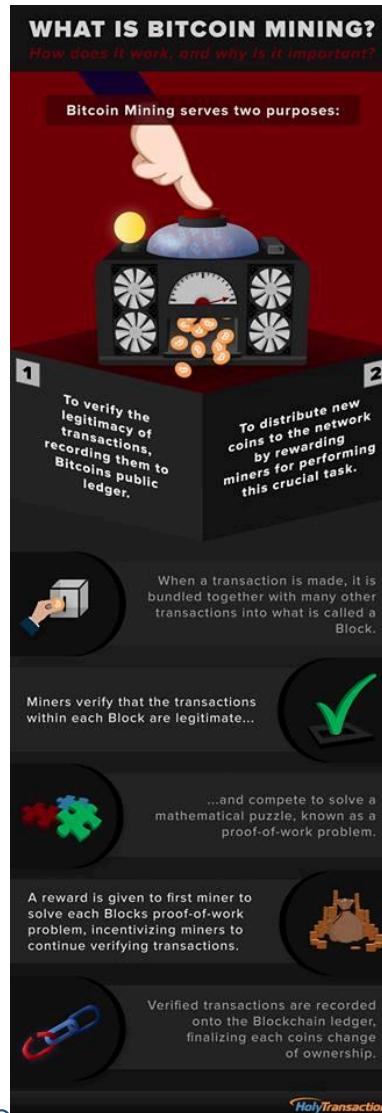
El proceso de consecución del nonce que resuelve el acertijo hash es lo que se conoce como minería bitcoin, dentro del cual se producen las operaciones de consenso distribuido antes explicadas. Los acertijos de minería están en el núcleo mismo de Bitcoin.

9. ¿QUÉ ES LA MINERÍA DE BITCOINS (CRIPTOMONEDAS)?

La selección aleatoria del nodo autorizado para crear un nuevo bloque se resuelve mediante el sistema de minería denominado Proof-of-Work (Prueba de Trabajo) (PoW). La idea clave detrás de Proof-of-Work es que se pueda aproximar la selección de un nodo arbitrario a, en su lugar, la selección de nodos en proporción de un recurso que esperamos que nadie pueda monopolizar. Si, por ejemplo, ese recurso es poder de cómputo, entonces es un sistema Proof-of-Work. Alternativamente, podría ser en proporción a la propiedad de la moneda, y se llama Proof-of-Stake (Prueba de Participación) (PoS). A pesar de que no se usa en Bitcoin, la Prueba de Participación es un modelo de minería alternativo legítimo y se usa en otras criptomonedas.

Todos estos sistemas buscan lograr el consenso descentralizado y la prevención del doble gasto y del ataque del 51%. Dependiendo del tipo de sistema que utilice la criptomoneda, cambiará la forma de minería.

9. ¿QUÉ ES LA MINERÍA DE BITCOINS (CRIPTOMONEDAS)?



10. ¿CÓMO MINAR CRIPTOMONEDAS?

Como hemos dicho antes la minería de criptomonedas depende del sistema de minería que utilice la cadena de bloques de la moneda digital a ser minada: sistema de Prueba de Trabajo (Proof-of-Work), sistema de Prueba de Participación (Proof-of-Stake) u otro, típicamente híbridos. Para todos estos sistemas de minería se han creado equipos, hardware, y esquemas comerciales de explotación minera que facilitan la incorporación de nuevos mineros a la red.

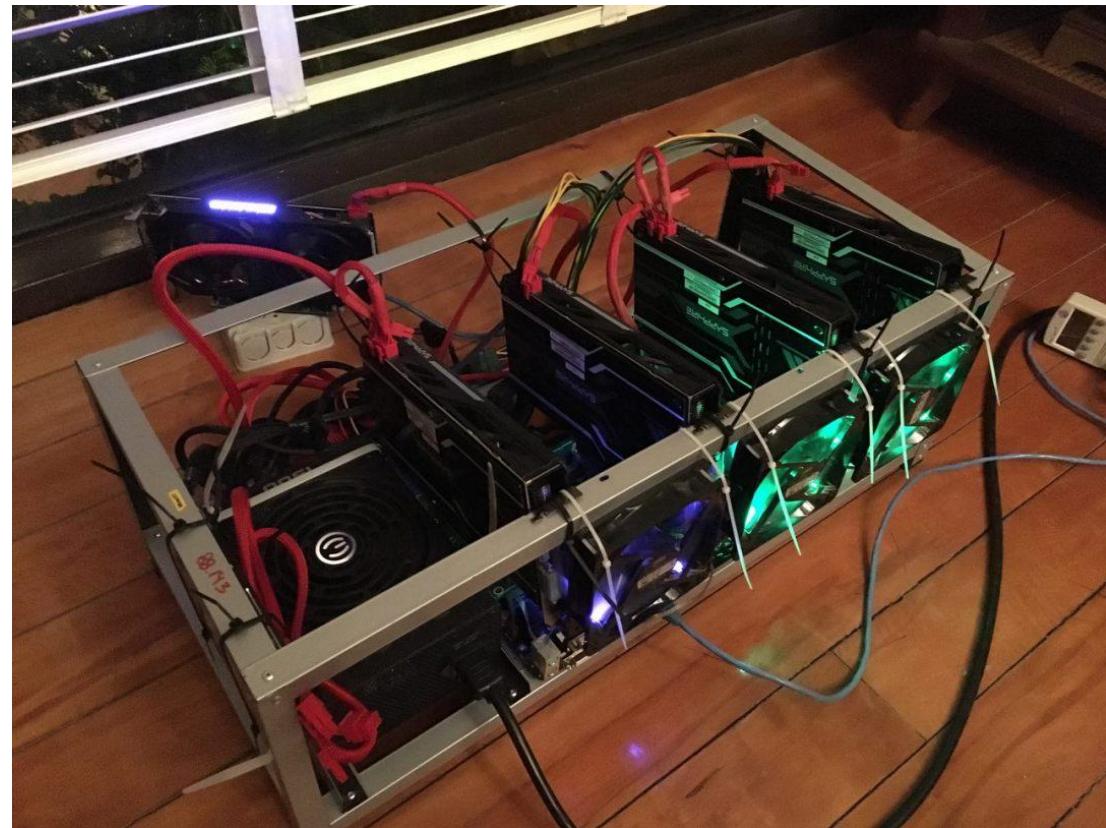
PROOF-OF-WORK

En el sistema de Prueba de Trabajo (PoW), los mineros utilizan procesadores, comerciales o especializados, para resolver los acertijos hash. Dependiendo del poder de procesamiento actual de la red de la criptomoneda, la dificultad para hallar el nonce determinará la cantidad de poder de computo necesario, así como el tipo de chip a utilizar.

10. ¿CÓMO MINAR CRIPTOMONEDAS?

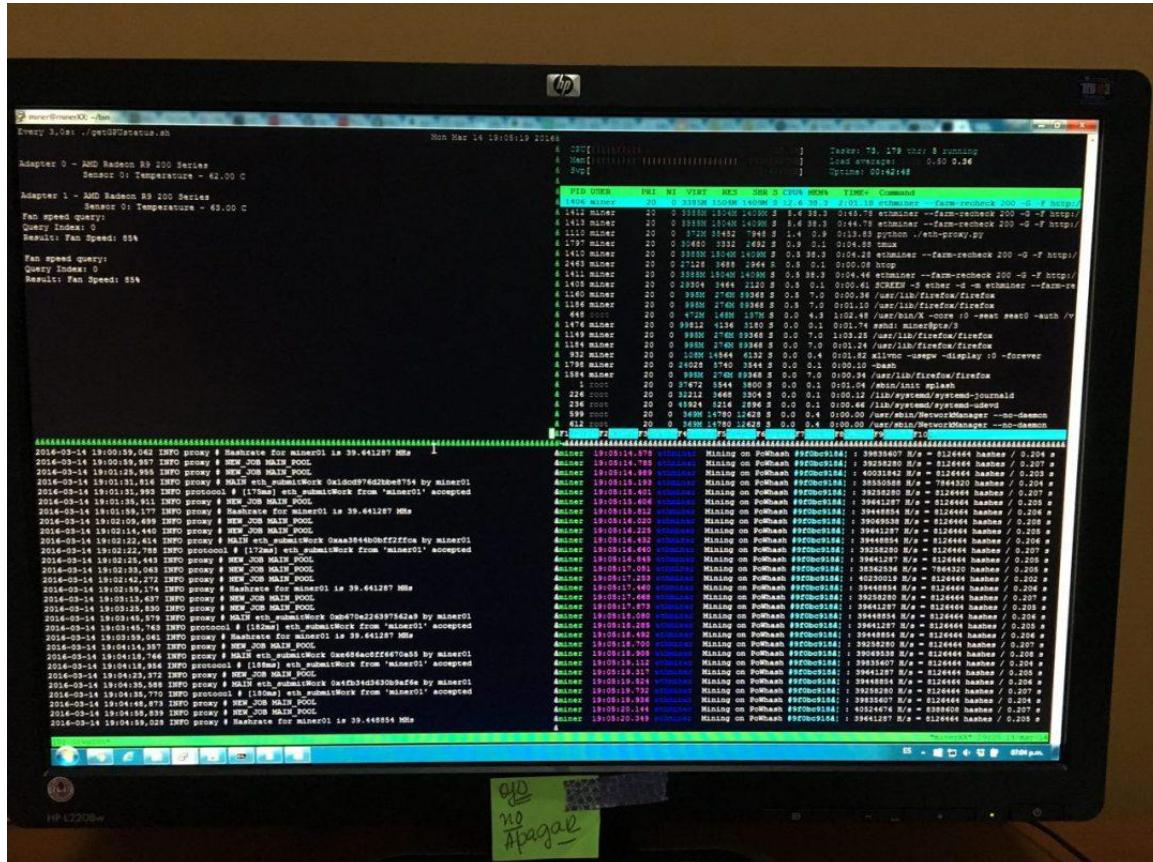
La minería de bitcoins, por ejemplo, ha utilizado chips de procesadores de computadora (CPU), tarjetas de video (GPU), chips programables (FPGA) y, actualmente, utiliza chips especializados (ASIC).

Para la minería con CPU, GPU y FPGA, los mineros deben realizar configuraciones especiales de estos chips en sus computadoras que les proporcionen un poder de cómputo competitivo en relación al poder de procesamiento total de la red de la criptomoneda que minan.



10. ¿CÓMO MINAR CRIPTOMONEDAS?

Además de esto, necesitan utilizar un software que les permita interactuar con la red de la criptomoneda para obtener los trabajos de los bloques a consolidar y enviar las soluciones que consigan.

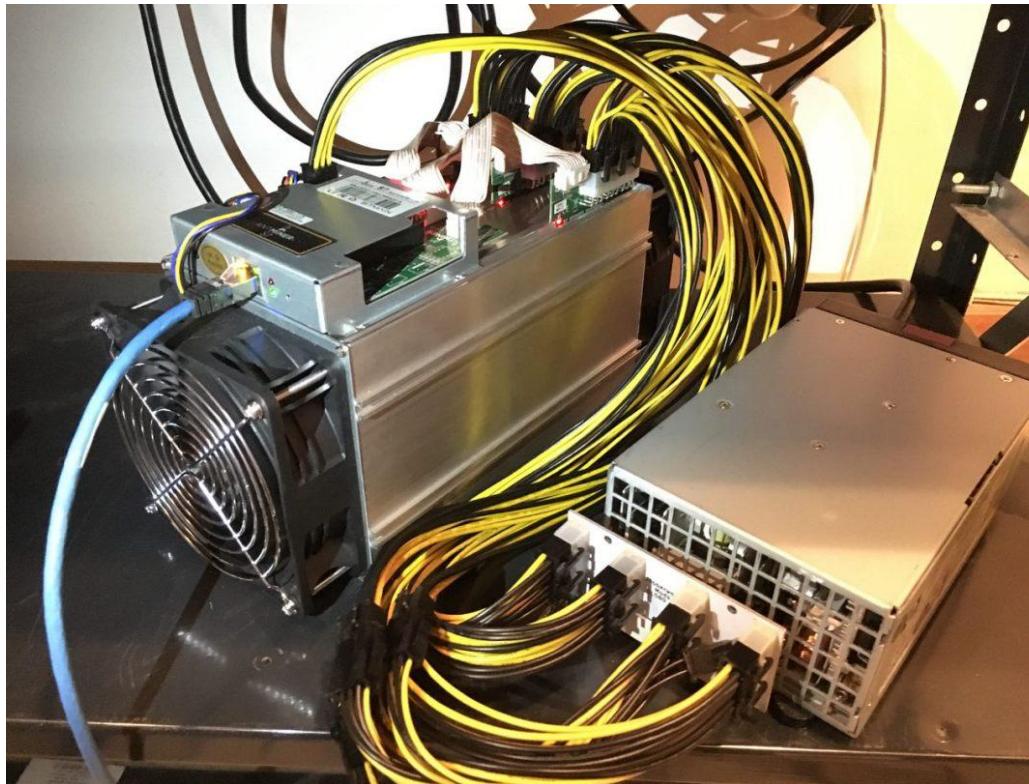


¿Qué son los Bitcoins? "On line"

Documentación recopilada por Mariano Hernando.

10. ¿CÓMO MINAR CRIPTOMONEDAS?

La minería con ASICs es mucho más sencilla. Los Circuitos Integrados de Aplicación Específica (ASIC, por sus siglas en inglés) son agrupados en tarjetas electrónicas que, a su vez, se conectan a una tarjeta de control que contiene el software de minería para dar vida a un minero modular. **ESPECIALMENTE DEDICADO A MINERIA.**



10. ¿CÓMO MINAR CRIPTOMONEDAS?

Gran porcentaje de las criptomonedas en el mercado utilizan el sistema de minado PoW con diferentes algoritmos de encriptación. Bitcoin, por ejemplo, utiliza SHA256; Litecoin, Scrypt; Ethereum, Ethash; Dash, X11; etc.

Los mineros se suelen situar en sitios donde el coste de la electricidad sea bajo y donde se puedan refrigerar bien las maquinas que hacen minería. Antes uno podía hacer minería en su casa con su ordenador de sobremesa en ratos libres y le compensaba económicamente, ahora la cosa ha cambiado mucho ya son mineros profesionales los que se dedican a ello

EMPRESA ESPECIALISTA EN MINEROS: <https://www.bitmain.com/>

10. ¿CÓMO MINAR CRIPTOMONEDAS?

PROOF-OF-STAKE

La Prueba de Participación (PoS) es una sistema de minado alternativo al PoW en el que se asigna un valor accionario a cada moneda que corresponde a la cantidad de monedas que recibirá el tenedor cuando haya transcurrido cierta cantidad de tiempo sin utilizar dicha moneda.

En este sistema, el valor obtenido va creciendo siempre que la moneda no sea utilizada. Si la moneda es usada, el valor accionario se reinicia.

La primera criptomoneda en utilizar este algoritmo fue Peercoin, que utiliza un híbrido entre PoW y PoS. Otras criptomonedas son: Qubits, Novacoin, Diamond, Nxt y muchas otras.

Además, Ethereum planea realizar un cambio de PoW a PoS para diciembre de 2016.

10. ¿CÓMO MINAR CRIPTOMONEDAS?

GRUPOS DE MINERÍA (MINING POOLS)

Los grupos de minería (mining pools) son una de las formas en que los mineros juntan sus recursos y comparten su poder de cálculo mientras dividen la recompensa por igual, en función a la cantidad de trabajo con la que contribuyeron en la obtención de un bloque.

La minería Bitcoin en grupos se inició cuando la dificultad de minado aumentó hasta el punto en el que podría llevar años para los mineros más lentos generar un bloque. La solución de los mineros a este problema fue agrupar sus recursos para que pudieran generar bloques más rápido y por lo tanto recibir una porción del bloque de recompensa Bitcoin sobre una base constante, en lugar de al azar una vez cada varios años.

El grupo de minería trabaja en conjunto para conseguir el mismo bloque, utilizando como recipiente de la recompensa la dirección de criptomonedas del responsable del grupo. El gerente se encarga de publicar los bloques a trabajar y luego de repartir las ganancias por bloque conseguido a los miembros, basado en la cantidad de trabajo que realizó cada uno, el cual es proporcional al poder de procesamiento que cada miembro controle.

Ver páginas <https://blockchain.info/pools> para el ALGORITMO sha-256 y para el ALGORITMO scrypt <https://www.litecoinpool.org/pools>

10. ¿CÓMO MINAR CRIPTOMONEDAS?

Por realizar este trabajo el responsable del grupo se queda con un porcentaje de las ganancias denominado cuota de grupo (pool fee). La cuota de grupo ronda comúnmente de 0-4% de las ganancias.

Slushpool, el primer grupo de minería creado, fue lanzado el 27 de noviembre de 2010. Desde entonces se ha vuelto una práctica habitual la minería en grupos, predominando casi absolutamente sobre la minería en solitario. Se ha extendido a la minería de muchas de las criptomonedas más conocidas: Bitcoin, Litecoin, Dash y Ethereum, entre otras.

Ventajas. Reducen la incertidumbre de minar un bloque y con ello, el riesgo económico; permiten a los mineros pequeños participar rentablemente y mantienen el software de validación de los mineros actualizado.

Desventajas. Fomentan la centralización de la red, desalientan a los mineros a correr nodos completos y hacen más engorroso (en algunos casos imposibilita) ejercer la voluntad de voto de los mineros ante cambios en la red.

10. ¿CÓMO MINAR CRIPTOMONEDAS?

MINERÍA EN LA NUBE (CLOUD MINING)

La minería de nube (cloud mining) o hashing de nube permite a los usuarios comprar capacidad de minado de hardware de centros de datos remotos, por un tiempo preestablecido acordado. Realmente, es un alquiler o arrendamiento de capacidad de cómputo que evita la adquisición de hardware y software de minado, consumo eléctrico y de ancho de banda, entre otros requerimientos de poseer un centro de minado.

Las ventajas de este esquema de minería están relacionadas con no tener que lidiar con los inconvenientes que los equipos de minado generan: calor y ruido excesivo, instalación de sistemas de ventilación, consumo eléctrico, compra y reparación de equipos, etc.

Las principales desventajas radican en las altas probabilidades de fraude al no poder verificar la existencia u operación del centro de datos y menor rentabilidad por el costo del servicio de minado; además, los contratos de minería en la nube contemplan el cese de operaciones o de pagos si el precio de la criptomoneda es demasiado bajo para cubrir los costos de operación, entre otros.

10. ¿CÓMO MINAR CRIPTOMONEDAS?

En la actualidad, existen compañías que ofrecen servicios de minería en la nube para varias de las criptomonedas más conocidas: Bitcoin, Litecoin, Dash y Ethereum, entre otras.

CEXio, la primera compañía de minería en la nube, se estableció en octubre del 2013. Actualmente existen muchas otras, siendo la más famosa Genesis Mining Y HASHFLARE.

Debido al alto grado de confianza que debe haber entre quien contrata el servicio y quien lo ofrece, este sistema se ha prestado para realizar múltiples estafas a lo largo de los años, por lo que se debe ser cauteloso a la hora de invertir en minería en la nube.

Vamos a ver ejemplos de minería en la nube en Hashflare y Génesis-mining.com

70% DE LA MINERIA DE BITCOIN ESTA BAJO EL CONTROL DE MINEROS CHINOS

11. Usos del Bitcoin Como Tecnología

Desde hace mucho tiempo se aprecia en muchos referentes del mundo financiero una frase que dice algo así: “la tecnología de bitcoin es interesante, pero no así la moneda o su uso como depósito de valor”... todo es interesante pero... para comprender a que se refieren, separemos a bitcoin en dos partes:

1) Bitcoin como moneda: se trata de la unidad digital que transferimos entre usuarios, que podemos utilizar como medio de pago o ahorro, y cuyo precio es definido por su oferta y demanda. Por estos días cotiza a US\$615 y se caracteriza por su independencia de Gobiernos y corporaciones, pero también por la volatilidad de su valor al compararlo con las monedas tradicionales, ... ojo con el concepto de independencia que no hay nada independiente.

2) Bitcoin como tecnología: es el denominado blockchain o cadena de bloques. Se trata de una base de datos distribuida que originalmente se pensó para registrar los movimientos de bitcoins de una cuenta a otra, pero que tiene gran potencial para otros usos, gracias a su almacenamiento descentralizado que no requiere de confianza en quienes la actualizan o custodian (difícil de falsificar, fácil de verificar). Algunos usos pueden ser: registro de propiedad de bienes tangibles o intangibles, contratos distribuidos, contratos inteligentes, patentes, timestamps, verificación de contenidos, derechos de autor, trazabilidad, etc.

11. Usos del Bitcoin Como Tecnología

La tecnología de cadenas de bloques de bitcoin sirve para múltiples aplicaciones. Sucede que mantener la base de datos distribuida tiene un costo, no solo de conectividad, sino que auditar y evitar falsificaciones en los registros implica poder de computo o procesamiento. Para que —pese al costo que implica—, se procesen los cambios en la base de datos, existe un sistema de incentivos, que consiste en repartir bitcoins a quienes aportan poder de procesamiento (informalmente llamados “mineros”). Es aquí donde bitcoin, la moneda y la tecnología, se relacionan y se necesitan mutuamente. En el futuro podemos tener diferentes alternativas a la actual. Si el incentivo o pago a los “mineros” no fuese en bitcoins, la descentralización no sería tal. Bitcoin dejaría de ser autosostenible y su funcionamiento dependería de factores externos, como jurisdicciones, permisos especiales, monedas tradicionales, bloqueos gubernamentales, etc. Su privacidad e inclusión estarían en juego, y la censura sería una posibilidad real.

Blockchain Use Cases: Comprehensive Analysis & Startups Involved



<https://azure.microsoft.com/es-es/solutions/blockchain/>

<https://azure.microsoft.com/es-es/documentation/templates/?term=blockchain>

[Blockchain - Ethereum Private Consortium](#)

This template fully automates the provisioning of necessary Azure resources like VMs, storage, network settings etc. as well as the configuration of Go Ethereum...



por [cavanes](#),
Última actualización: 20/09/2016

[Secure Ubuntu by Trailbot](#)

This template provides a Ubuntu VM which comes with a special demon called Trailbot Watcher that monitors system files and logs, triggers Smart Policies upon mo...



por [Trailbot](#),
Última actualización: 09/08/2016

[Viacoin Blockchain on Ubuntu](#)

This template deploys a Viacoin node on a Ubuntu virtual machines.



por [Romano](#),
Última actualización: 12/07/2016

[NXT blockchain platform on Ubuntu](#)

Nxt is an open source second generation blockchain that provides tools for a decentralized financial platform



por [bcdev-](#),
Última actualización: 28/03/2016

[Bitswift Blockchain on Ubuntu](#)

This template deploys a Bitswift node on a Ubuntu virtual machines. Bitswift information can be found at <https://bitcointalk.org/index.php?topic=922982.msg1...>



por [Steven](#),
Última actualización: 26/03/2016

[DigiByte on Ubuntu](#)

This template deploys a DigiByte node on a Ubuntu virtual machines.



por [DigiByte Payment Network](#),
Última actualización: 26/03/2016

[Blocknet Blockchain on Ubuntu](#)

This template deploys a Blocknet node on a Ubuntu virtual machines. Blocknet services include enabling multi-blockchain services to be delivered to devices th...



por [Steven](#),
Última actualización: 24/03/2016

[Jumbucks Blockchain on Ubuntu](#)

This template deploys a Jumbucks node on a Ubuntu virtual machines.



por [Julian Yap](#),
Última actualización: 21/03/2016

[Vcash on Ubuntu](#)

This template deploys a Vcash node onto an Ubuntu Virtual Machine.



por [John Connor](#),
Última actualización: 20/03/2016

[Manifold Platform Endpoint on CentOS](#)

This template installs the Manifold Platform Blockchain as a Service Endpoint on a CentOS VM.



por [Tyler Pinckard](#),
Última actualización: 17/03/2016

[Influx Blockchain on Ubuntu](#)

This template deploys a Influx node on a Ubuntu virtual machines. Influx services include VPS hosting, payment API service for 3rd parties, and SuperNET Multi-Gatew...



por [Steven](#),
Última actualización: 15/03/2016

[Monero Full Node on Ubuntu](#)

This template deploys a Monero node on an Ubuntu VM. Monero is primarily focused on transactional privacy for users, and is best-suited to developers loo...



por [The Monero Project](#),
Última actualización: 15/03/2016

BLOCKCHAIN TECHNOLOGY APPLICATIONS



CRYPTO-TECHNOLOGY LANDSCAPE

11. US

APPLICATIONS



MIDDLEWARE SERVICES



ANCILLARY SERVICES



INFRASTRUCTURE & PLATFORMS



¿Qué usos, aparte de la moneda, se te ocurren que puede utilizarse la tecnología bitcoin?

(Un caso de uso de la tecnología, por ejemplo es: votaciones)

En la industria que trabajas, ¿qué procesos piensas que puede cambiar?

11. Usos del Bitcoin Como Tecnología

Acciones emitidas por una compañía. Esto significa que las empresas pueden definir una etiqueta identificatoria a un bitcoin y lo pueden vender a aquellos que quieran invertir en la compañía como si fuese una acción. Esta acción, puede ser vendida, y transferida a otras personas simplemente mediante una simple transacción de bitcoin. Compañías como CoinPrism y ChromaWallet permiten hacer esto.

Sistema de Votación, en el cuál el votante hace una transacción hacia la dirección pública de su candidato preferido. Hay algunas soluciones en desarrollo, como por ejemplo Bitcongress o Agora, que ofrecen un sistema en el que facilitan la administración de las votaciones.

Para diseñar contratos inteligentes, es decir acuerdos digitales que se ejecuten cuando se cumplan ciertas condiciones. Un ejemplo, son los contratos de herencia, que se pueden programar para que los herederos reciban la información para acceder a los fondos, solo cuando se cumplen determinadas condiciones.

11. Usos del Bitcoin Como Tecnología

Certificación de cierta información. Por ejemplo, la certificación de origen de un producto. En Australia, ya están usando un sistema de certificación de vino, usando la tecnología Bitcoin. Para esto, a cada botella le corresponde una dirección pública de una billetera creada por el viñedo y que contiene una fracción de bitcoin. Cuando se le entrega la botella al distribuidor, el viñero realiza la transacción de esa fracción de bitcoin a la billetera del distribuidor. Cuando el distribuidor vende ese vino a un cliente, también realiza la transacción del bitcoin al cliente y así sucesivamente. Un comprador puede verificar la veracidad de la botella de vino revisando el historial de transacciones de la fracción de bitcoin.

<http://criptonoticias.com/aplicaciones/blockchain-junto-iot-revolucionaran-multiples-areas/>
LA INTERNET DE LAS COSAS IOT Y LA BLOCKCHAIN

Ejemplo banco: <https://www.wb21.com/> permite ingresos en Bitcoin.
<https://www.wb21.com/fees/>

11. Usos del Bitcoin Como Tecnología

Otro uso de la tecnología bitcoin es en la generación de un registro de personas. Hay varios proyectos en desarrollo, siendo el de Christopher Ellis el más reconocido. El proyecto es de código abierto, es decir que cualquier persona o institución lo puede utilizar o editar, y tiene como objetivo crear una prueba de existencia de una persona y grabarlo en la cadena de bloques, de forma tal que nadie pueda cambiarlo.

Otros usos como tickets para eventos, puntos de recompensa o fidelidad, etc.

FAVORECIDOS CLARAMENTE POR LA BLOCKCHAIN ES LA INDUSTRIA DE CONTENIDOS DIGITALES: AUDIO, VIDEO, TELEVISION, BLOCKCHAIN APLICADO A LOS DERECHOS DE AUTOR:

<http://www.diariobitcoin.com/index.php/2016/09/13/iniciativa-musical-recauda-25-millones-por-uso-de-blockchain-aplicado-a-derechos-de-autor/>

<http://www.diariobitcoin.com/index.php/2016/09/07/conozca-kashcoin-la-criptomoneda-disenada-para-la-industria-de-la-musica/>

12. Bitcoin vs otras Criptomonedas.

<https://coinmarketcap.com/>

Litecoin <https://coinmarketcap.com/currencies/litecoin/>

Dogecoin <https://coinmarketcap.com/currencies/dogecoin/>

Monero <https://coinmarketcap.com/currencies/monero/>

Steem <https://coinmarketcap.com/currencies/steem/>

Dash <https://coinmarketcap.com/currencies/dash/>

Ripple <https://coinmarketcap.com/currencies/ripple/>

DigixDAO <https://coinmarketcap.com/assets/digixdao/>

Factom <https://coinmarketcap.com/currencies/factom/>

NEM <https://coinmarketcap.com/currencies/nem/>

ASSET <> CURRENCIES

12. Bitcoin vs otras Criptomonedas. Asset

¿Qué es un Asset/Activo en criptomonedas?. Son lo que se conoce comoMetaCoins, Altchain/Parachains o Appcoins

Metacoins – que utilizan la cadena de bloques de Bitcoin, pero codifican sus propios metadatos para nuevas aplicaciones.

Altchains/Parachain – que utiliza su propia cadena de bloques independiente de Bitcoin, pero no tiene como objetivo ser un activo monetario. Pueden ser activos de inversión, pero sus Token se utilizan para aplicaciones.

AppCoin – pueden compartir o no la cadena de bloques de Bitcoin. Son activos derivados de un sistema basado en criptomonedas con una aplicación. El activo se representa por un Token. Con ese token, que tiene función de clave, el usuario tiene acceso al uso de la aplicación y a la vez se convierten en una herramienta para recaudar fondos para los desarrolladores de dicha aplicación.

¿Qué son las Colored Coins basada en Bitcoin?

Las Colored Coins, que se traduciría como Monedas de Colores (aunque usaremos el término en inglés), son bitcoins (más concretamente una pequeña fracción de un bitcoin, un satoshi) que han sido ‘coloreados’ mediante la introducción de un código específico, con el fin de representar a otro activo. Este activo puede ser una acción de una empresa, un lingote de oro, un dólar o un euro, un derivado, el título de propiedad de una casa, o incluso puede representar un voto, es decir, puede ser cualquier cosa del mundo real.

Las Colored Coins añaden versatilidad a Bitcoin y abren un amplio abanico de posibilidades, porque convierte estos bitcoins codificados como ‘coloreados’ en tokens con un valor secundario añadido que pueden ser usados como cualquier cosa para la que quieran ser usados, y hacer uso de la red Bitcoin para asegurarlos y transferirlos.

12. Bitcoin vs otras Criptomonedas. FORK, HARD FORK, SOFT FORK

Un fork o bifurcación es un término que se utiliza a menudo en el desarrollo de software y que significa clonar un código fuente. En Bitcoin, un fork o bifurcación puede significar, por lo tanto, un proyecto que clona el código fuente de Bitcoin, para tomarlo como base e introducir en él los cambios que crea conveniente.

– Fork o bifurcación accidental. Estos fork o bifurcaciones pueden ocurrir, como su propio nombre indica, de manera accidental (fork o bifurcación accidental) cuando los desarrolladores principales de Bitcoin cometan un error en la actualización de código de la criptomoneda.

12. Bitcoin vs otras Criptomonedas. FORK, HARD FORK, SOFT FORK

- **Hard fork o bifurcación dura / Soft fork o bifurcación blanda** se refiere a cuando se introduce conscientemente cambios o implementaciones en el código Bitcoin.
- Un **soft fork** introduce cambios en el software de Bitcoin, de tal manera que el software actualizado es compatible con las otras versiones de software más antiguas, por lo que ambas versiones pueden coexistir en la misma red Bitcoin.
- Un **hard fork** introduce cambios en el software, de tal manera que el software actualizado no es compatible con otras versiones de software. En consecuencia, un hard fork es un cambio en las reglas de consenso en el cual bloques inválidos bajo las reglas viejas podrían ser válidos bajo las nuevas reglas.

12. Bitcoin vs otras Criptomonedas. CONTRATOS INTELIGENTES

¿Qué son los contratos inteligentes o smart contracts? En esencia el término contrato inteligente (smart contract) se refiere a cualquier tipo de contrato entre dos o más partes, que es capaz de ejecutarse y hacerse cumplir por sí mismo, de manera autónoma y automática. Además, las partes de un contrato inteligente pueden ser tanto personas como máquinas, lo que abre una ventana al Internet de las Cosas (Internet of Things – IoT).

Usos de los contratos inteligentes: Préstamos, Depósito en garantía, Controles de gasto Y Herencias y donaciones.

Algunos protocolos y plataformas de contratos inteligentes o smart contracts:

- [BitHalo](#)
- [BlackHalo](#)
- [Codius](#)
- [Counterparty](#)
- [Ethereum](#)
- [RootStock](#)

13. ¿Qué es Ethereum?

Ethereum es una Blockchain o Tecnología de Contabilidad Distribuida (DTL) con un lenguaje de programación Turing completo integrado, una computadora blockchain, que permite que cualquiera pueda escribir contratos inteligentes y aplicaciones descentralizadas simplemente escribiendo la lógica en unas pocas líneas de código.

Ethereum – Plataforma de Aplicaciones Blockchain



13. ¿Qué es Ethereum?

El protocolo Ethereum fue concebido originalmente como una versión mejorada de la criptomoneda Bitcoin, para superar las limitaciones de su lenguaje de programación, proporcionando características avanzadas tales como custodia sobre la blockchain, límites de retiro, contratos financieros, mercado de juegos de azar y similares a través de un lenguaje de programación muy generalizado.

En Ethereum, una versión básica de Namecoin, la base de datos de registro de nombres descentralizada, DNS de internet, se puede escribir en dos líneas de código, y otros protocolos como monedas y sistemas de reputación se pueden construir en menos de veinte líneas. Contratos inteligentes, “cajas” criptográficas que contienen valor y sólo se desbloquean si se cumplen ciertas condiciones, también pueden ser incorporados encima de la plataforma, con mucho más poder que la ofrecida por el script de Bitcoin debido al poder agregado del Turing completo que es como esta programado.

13. ¿Qué es Ethereum?

El protocolo Ethereum no “soporta” cualquiera de las aplicaciones directamente, pero la existencia de un lenguaje de programación Turing completo permite que contratos arbitrarios teóricamente se puedan crear para cualquier tipo de transacción o aplicación. Lo que es más interesante de Ethereum, sin embargo, es que el protocolo Ethereum se mueve mucho más allá de la moneda. Protocolos alrededor de almacenamiento de archivos descentralizados, computación descentralizada y mercados de predicción descentralizados, entre docenas de otros conceptos similares, tienen el potencial para aumentar sustancialmente la eficiencia de la industria computacional, y proporcionar un gran impulso a otros protocolos peer-to-peer adicionando por primera vez una capa económica. En realidad hay una variedad considerable de aplicaciones que no tienen nada que ver con el dinero en absoluto, Ethereum sería un gestor de aplicaciones y sobre el mismo correrían contratos inteligentes y dao, aplicaciones autónomas descentralizadas.

Hardfork / Non-fork de ethereum revisamos en fork.ethstats.net
<https://cryptowatch.es/kraken/ethusd/1d>
<https://cryptowatch.es/kraken/ethbtc/1w>

Problema de DAO & Vitalik Buterin

13. ¿Qué es Ethereum?

¿QUÉ ES ETHER? ETH

Ethereum Criptomoneda Blockchain

Símbolo de la criptomoneda Ether de Ethereum

Ether ETH es la criptomoneda de Ethereum, el combustible que impulsa esta plataforma de aplicaciones distribuidas. Es una criptomoneda utilizada por los clientes de la plataforma Ethereum para realizar pagos a otras personas o a máquinas que ejecutan operaciones solicitadas. Es decir, Ether es el incentivo que asegura que los desarrolladores escriban aplicaciones de calidad (la codificación innecesaria cuesta más) y que la red permanezca saludable (la gente es recompensada por los recursos aportados).



[http://www.the-blockchain.com/docs/Ethereum white paper-a next generation smart contract and decentralized application platform-vitalik-buterin.pdf](http://www.the-blockchain.com/docs/Ethereum%20white%20paper-a%20next%20generation%20smart%20contract%20and%20decentralized%20application%20platform-vitalik-buterin.pdf)

13. ¿Qué es Ethereum?

La oferta total de Ether y su tasa de emisión fue decidida en la preventa de 2014. Los datos claves de aquella preventa son los siguientes:

60 millones de Ether fueron creados para los contribuyentes de la preventa.

- 12 millones fueron creados para el fondo de desarrollo, la mayoría de ellos fue a los primeros contribuyentes y a los desarrolladores y el resto a la Fundación Ethereum.
- 5 Ether son creados por cada bloque (cada 15-17 segundos) para los mineros de los bloques.
- 2-3 Ether son algunas veces enviados a otros mineros si ellos fueron capaces de encontrar una solución pero su bloque no fue incluido (llamada recompensa tío/tía).
- De acuerdo a los términos acordados por todas las partes en la preventa de 2014, la emisión de Ether está limitada a 18 millones de Ether por año (25 % de la oferta inicial).

Ethereum cambiará su esquema de minado de Prueba de Trabajo (PoW) a Prueba de Participación (PoS) bajo el nombre clave Casper. Hombre clave Vitalik Buterin

13. ¿Qué es Ethereum?

¿QUÉ ES GAS?

Con el fin de evitar bucles infinitos accidentales, hostiles, u otro desperdicio computacional en el código, cada transacción es obligada a establecer un límite al número de pasos computacionales de ejecución de código que ella puede utilizar. La unidad fundamental de computación es “gas”. Por lo general, un paso computacional cuesta 1 gas, pero algunas operaciones cuestan cantidades más altas de gas porque son más costosas computacionalmente, o porque aumentan la cantidad de datos que deben ser almacenados como parte del estado. También hay una tarifa de 5 gas por cada byte en los datos de transacción.

La intención del sistema de comisiones es obligar a un atacante a pagar proporcionalmente por cada recursos que consume, incluyendo computación, ancho de banda y almacenamiento. Por lo tanto, cualquier operación que conduzca a la red a consumir una mayor cantidad de cualquiera de estos recursos debe tener una comisión de gas más o menos proporcional al incremento.

Fuente: [Ethereum white paper](#)

13. ¿Qué es Ethereum?

¿QUÉ Y QUIEN ES LA FUNDACION Ethereum?

<https://www.ethereum.org/foundation>

Mission and Vision Statement

The Ethereum Foundation's mission is to promote and support research, development and education to bring decentralized protocols and tools to the world that empower developers to produce next generation decentralized applications (dapps), and together build a more globally accessible, more free and more trustworthy Internet.



ETHERUM

13. ¿Qué es Ethereum?

ESTA PERSONA ES Y SERÁ MUY IMPORTANTE

VITALIK BUTERIN

IN ETHEREUM WE TRUST



BITCOIN POPULARITY WORLDWIDE

**NORTH
AMERICA**

30k+
transactions
per day

**SOUTH
AMERICA**

2k+
transactions
per day

AFRICA

1k+
transactions
per day

EUROPE

5k+
transactions
per day

ASIA

160k+
transactions
per day

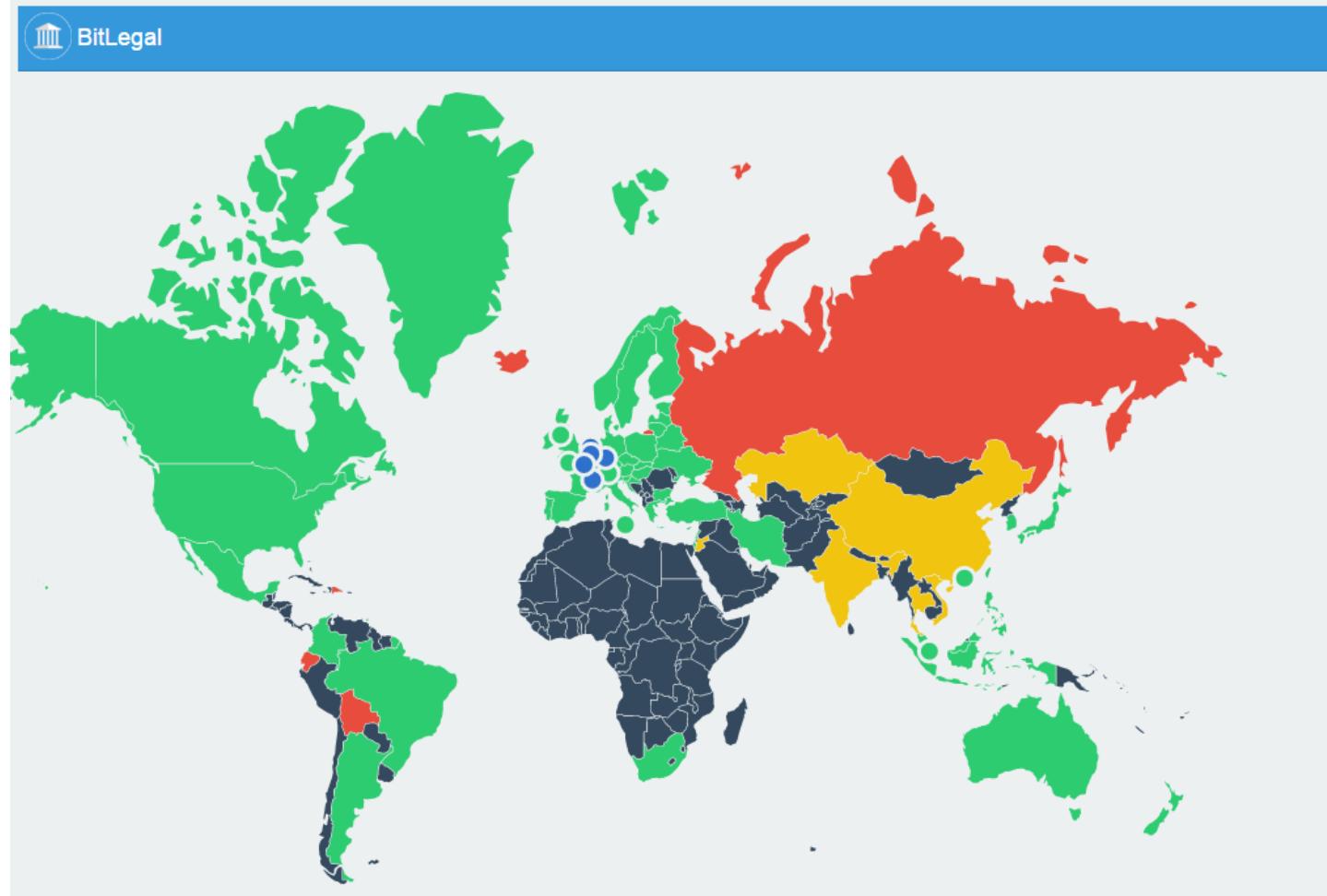
OCEANIA

3k+
transactions
per day



15. ¿Cómo es la regulación de Bitcoin en el Mundo? (1)

Web: <http://bitlegal.io/>
tienes un mapa legislativo del Bitcoin a nivel mundial así como un recopilatorio de todas las novedades legislativas a nivel mundial.



15. ¿Cómo es la regulación de Bitcoin en el Mundo? (2)

En <http://bitlegal.io/list.php> está la lista de países y la situación general del Bitcoin y las Criptomonedas en los mismos, países problemáticos u hostiles serían: China, Rusia, Bolivia, India, Tailandia, Vietnam, Ecuador, ...

Noticias relacionadas con la unión europea las podemos obtener a partir de la consulta:
<http://bitlegal.io/?s=european+union>

Noticias de regulación y legislativas en castellano en <http://criptonoticias.com/?s=regulacion> y en inglés <http://www.coindesk.com/regulation/>:

<http://criptonoticias.com/regulacion/espana-lider-europeo-inversiones-blockchain-gracias-resuestas-ministerio-hacienda/>
<http://criptonoticias.com/regulacion/mineros-bitcoins-criptomonedas-impuestos-espana/>
<http://criptonoticias.com/regulacion/congreso-eeuu-busca-regulaciones-favorables-tecnologia-blockchain/>
<http://criptonoticias.com/regulacion/australia-emprendera-regulaciones-contra-financiamiento-terrorismo-monedas-digitales/>
<http://criptonoticias.com/regulacion/comision-europea-regulacion-criptomonedas-lavado-dinero-terrorismo/>
<http://www.coindesk.com/research/regulation-report/> (reporte regulatorio completo por 99\$)
<http://www.coindesk.com/eus-top-cop-launches-digital-currency-working-group/>
<http://www.coindesk.com/bank-of-england-fintech-accelerator-eyeing-more-blockchain-projects/>

A nivel de mercados financieros tenemos. ESMA Discussion Paper
The Distributed Ledger Technology Applied to Securities Markets
https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt_0.pdf

15. ¿Cómo es la regulación de Bitcoin en el Mundo? (3)

La LICENCIA de utilización del Bitcoin es la MIT License, el texto de la MIT License diferencia entre tres puntos:

- Condiciones, la condición es que la nota de copyright y la parte de los derechos se incluya en todas las copias o partes sustanciales del Software. Esta es la condición que invalidaría la licencia en caso de no cumplirse.
- Derechos, los derechos son muchos: sin restricciones; incluyendo usar, copiar, modificar, integrar con otro Software, publicar, sublicenciar o vender copias del Software, y además permitir a las personas a las que se les entregue el Software hacer lo mismo.
- Limitación de responsabilidad, finalmente tiene un *disclaimer* o nota de limitación de la responsabilidad habitual en este tipo de licencias.

16. Algunas webs relevantes en el mundo Bitcoin.

- www.criptonoticias.com
- www.coinmarketcap.com
- www.coindesk.com
- [**Bitlegal.io**](http://Bitlegal.io)
- [**www.kraken.com**](http://www.kraken.com)
- [**www.diariobitcoin.com**](http://www.diariobitcoin.com)
- www.circle.com
- www.r3cev.com
- www.bittrex.com
- www.poloniex.com
- [**https://www.wb21.com/**](https://www.wb21.com/)

¿QUÉ SON LOS BITCOINS? ON LINE

mhernando@grupobme.es

tsai0835@gmail.com

Mariano Hernando