

Bitcoin: Un viaje inesperado

Francisco Rodríguez-Henríquez
Departamento de Computación



Top Tamulipas-CINVESTAV, veintisiete de septiembre de 2018

Dinero



- La importancia del dinero en una sociedad es tan alta, que a través de los siglos y en todas las latitudes no hubo gran civilización que no lo utilizara



- La importancia del dinero en una sociedad es tan alta, que a través de los siglos y en todas las latitudes no hubo gran civilización que no lo utilizara
- Para que algo funcione eficazmente como dinero, debe ser fácil de estandarizar, permitiendo que su valor sea una tarea simple por determinar; debe ser intercambiable entre individuos, divisible, resistente, fácil de portar pero al mismo tiempo difícil de falsificar.

Funciones del Dinero



Sin importar cuál sea su materialización, en la economía de una sociedad el dinero cumple con tres funciones principales:

Funciones del Dinero



Sin importar cuál sea su materialización, en la economía de una sociedad el dinero cumple con tres funciones principales:

- El dinero como un **medio de cambio**

Funciones del Dinero



Sin importar cuál sea su materialización, en la economía de una sociedad el dinero cumple con tres funciones principales:

- El dinero como un **medio de cambio**
- El dinero como **unidad de medida**

Funciones del Dinero



Sin importar cuál sea su materialización, en la economía de una sociedad el dinero cumple con tres funciones principales:

- El dinero como un **medio de cambio**
- El dinero como **unidad de medida**
- El dinero como **depósito de valor**

Ventajas/desventajas del dinero en efectivo



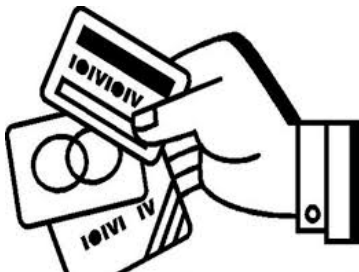
- **Ventajas:**

- ▶ Anonimato
- ▶ En su contexto de validez se acepta en cualquier lugar con un manejo simple
- ▶ es fácilmente transferible y permite dar cambio

- **Desventajas:**

- ▶ El propietario del papel moneda es quien lo porta
- ▶ Es difícil y/o peligroso transportar grandes cantidades de dinero
- ▶ Las transacciones deben realizarse en persona

Ventajas/desventajas del dinero plástico



● **Ventajas:**

- ▶ permite transacciones de grandes sumas de dinero
- ▶ fácil portabilidad, uso seguro
- ▶ La transacción puede realizarse aún si el comprador no está presente
- ▶ Se puede obtener dinero en efectivo a partir de éste
- ▶ permite revocar transacciones

● **Desventajas:**

- ▶ No permite el anonimato del comprador
- ▶ Requiere conexión en línea
- ▶ No es transferible entre particulares

Ventajas/desventajas del dinero electrónico



● **Ventajas:**

- ▶ Permite diversos grados de anonimato
- ▶ Transferible, divisible
- ▶ No está asociado a ninguna entidad bancaria o gobierno de ningún país
- ▶ Puede ser utilizado para descentralizar actividades comerciales

● **Desventajas:**

- ▶ Las transacciones suelen involucrar un esfuerzo computacional grande
- ▶ puede ser empleado en negocios turbios
- ▶ Hasta el momento muestra una gran volatilidad

Características deseables del dinero electrónico



- 1 Debe ser **independiente** de los medios electrónicos

Características deseables del dinero electrónico



- 1 Debe ser **independiente** de los medios electrónicos
- 2 Debe ser **seguro**

Características deseables del dinero electrónico



- 1 Debe ser **independiente** de los medios electrónicos
- 2 Debe ser **seguro** Debe resolver el problema del **doblo gasto**

Características deseables del dinero electrónico



- 1 Debe ser **independiente** de los medios electrónicos
- 2 Debe ser **seguro** Debe resolver el problema del **doblo gasto**
- 3 Debe garantizar **anonimato**

Características deseables del dinero electrónico



- 1 Debe ser **independiente** de los medios electrónicos
- 2 Debe ser **seguro** Debe resolver el problema del **doble gasto**
- 3 Debe garantizar **anonimato**
- 4 Debe ser **transferible**

Características deseables del dinero electrónico



- 1 Debe ser **independiente** de los medios electrónicos
- 2 Debe ser **seguro** Debe resolver el problema del **doble gasto**
- 3 Debe garantizar **anonimato**
- 4 Debe ser **transferible**
- 5 Debe ser **divisible**

Características deseables del dinero electrónico



- 1 Debe ser **independiente** de los medios electrónicos
- 2 Debe ser **seguro** Debe resolver el problema del **doble gasto**
- 3 Debe garantizar **anonimato**
- 4 Debe ser **transferible**
- 5 Debe ser **divisible**
- 6 Debe ser **eficiente**

Dinero digital: Primeras propuestas



- Las primeras construcciones de sistemas monetarios electrónicos fueron planteadas por **David Chaum** en los años ochentas del siglo pasado
- Para evitar la reutilización de las monedas electrónicas, **Chaum** propuso que cada moneda tuviera un identificador único y que una entidad Banco estuviese a cargo de verificar la correctitud del sistema de pagos

Dinero digital: Primeras propuestas



1

¹M. en C. Efrén Clemente Cuervo: "Implementación de un Monedero Digital Móvil", CINVESTAV, **noviembre de 2005**. Supervisor: Dr. Francisco Rodríguez-Henríquez

Dinero digital: Primeras propuestas



¹M. en C. Efrén Clemente Cuervo: “Implementación de un Monedero Digital Móvil”, CINVESTAV, **noviembre de 2005**. Supervisor: Dr. Francisco Rodríguez-Henríquez

Críticas al dinero electrónico centralizado



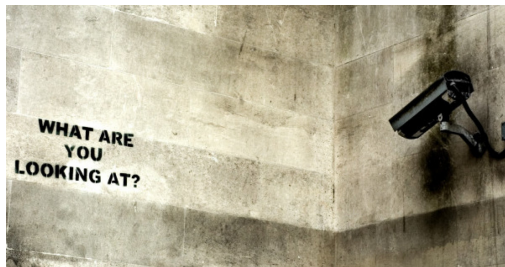
- 1 Puede ser utilizado para actividades ilícitas

Críticas al dinero electrónico centralizado



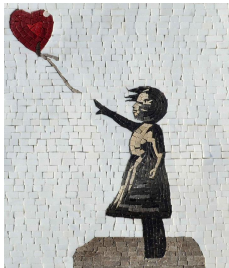
- 1 Puede ser utilizado para actividades ilícitas
- 2 Resulta extremadamente difícil evitar el problema del **doblo gasto**

Críticas al dinero electrónico centralizado



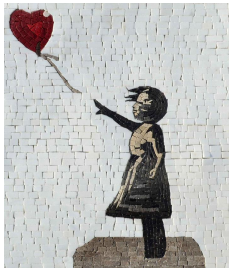
- 1 Puede ser utilizado para actividades ilícitas
- 2 Resulta extremadamente difícil evitar el problema del **doblo gasto**
- 3 La entidad **Banco** tiene un poder casi total en el sistema [**¡¡jital y como ocurre con el dinero plástico!!**]

Resultado de las críticas al dinero electrónico centralizado



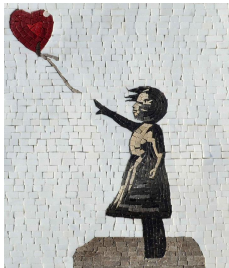
- El dinero electrónico centralizado nunca logró consolidarse como una alternativa real en el sistema monetario mundial

Resultado de las críticas al dinero electrónico centralizado



- El dinero electrónico centralizado nunca logró consolidarse como una alternativa real en el sistema monetario mundial
- Hubo poco interés por parte de los bancos comerciales en promover el concepto del dinero electrónico

Resultado de las críticas al dinero electrónico centralizado



- El dinero electrónico centralizado nunca logró consolidarse como una alternativa real en el sistema monetario mundial
- Hubo poco interés por parte de los bancos comerciales en promover el concepto del dinero electrónico
- También hubo un rechazo social de organizaciones activistas tales como el movimiento [ciberpunk](#)

Resultado de las críticas al dinero electrónico centralizado



- En 2010 el gobierno de EUA ordenó a las principales compañías de tarjetas de crédito y pagos electrónicos (VISA, MasterCard, PayPal, etc.) no aceptar los donativos que fuesen dirigidos a la organización [Wikileaks](#)
- Afortunadamente para [Wikileaks](#) la cripto-moneda **bitcoin** ya había iniciado su cabalgata en el mundo digital

Resultado de las críticas al dinero electrónico centralizado



Julian Assange
@JulianAssange

Follow

My deepest thanks to the US government, Senator McCain and Senator Lieberman for pushing Visa, MasterCard, Payal, AmEx, Mooneybookers, et al, into erecting an illegal banking blockade against @WikiLeaks starting in 2010. It caused us to invest in Bitcoin -- with > 50000% return.



10:05 AM - 14 Oct 2017

Dinero electrónico distribuido

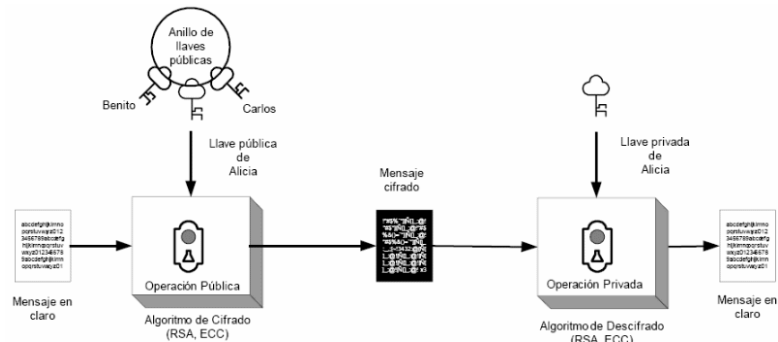


- Todos los modelos de dinero electrónico propuestos hasta antes de 2008 fueron **centralizados**
- Memorablemente, en 2008, **Satoshi Nakamoto** publica el artículo parteaguas: “**Bitcoin: A Peer-to-Peer Electronic Cash System**”, donde Nakamoto combina varios conceptos de propuestas previas para lograr una versión **distribuida** del dinero electrónico

Ingredientes criptográficos de Bitcoin



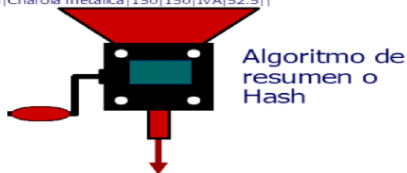
Criptografía de llave pública



Funciones picadillo

Cadena Original

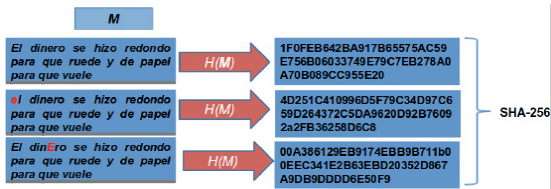
```
[[A|1|2005-09-02T16:30:00|1|ISP900909Q88|Industrias del  
Sur Poniente, S.A. de C.V.|Alvaro Obregón|37|3|Col. Roma  
Norte|México|Cauhtémoc|Distrito Federal|México|06700|  
Pino Suarez|23|Centro|Monterrey|Monterrey|Nuevo León|  
México|95460|CAUR390312S87|Rosa María Calderó|Uriegas|  
Topochico|52|Jardines del Valle|Monterrey|Monterrey|Nuevo  
León|México|95465|10|Caja|Vasos decorados|20|200|1|  
pieza|Charola metálica|150|150|IVA|52.5|]
```



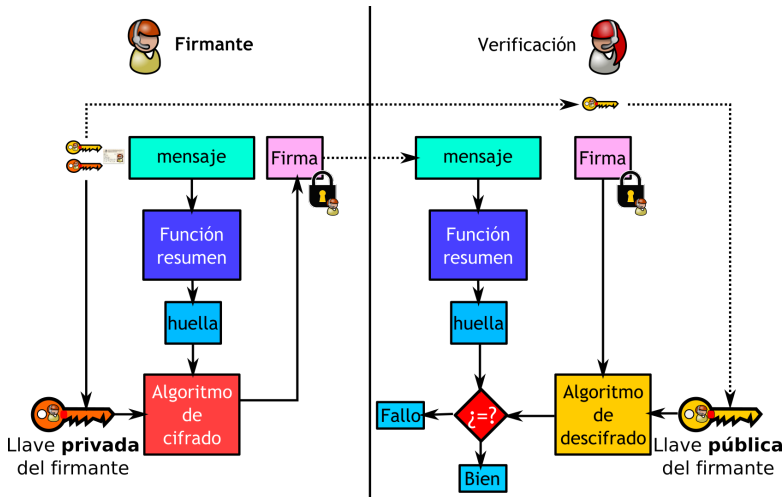
```
8a a2 b6 17  
94 44 27 35  
36 97 e6 94  
a2 e3 5a 07
```

Resumen o Hashing

Funciones picadillo



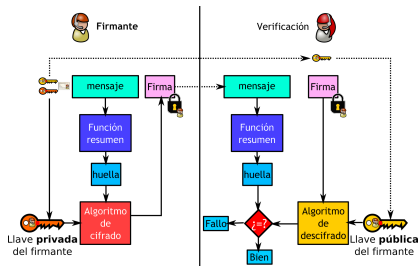
Firma digital



Firma digital

En resumen, a diferencia de la firma autógrafa tradicional donde sólo se verifica la autenticidad del signatario, para un esquema de **firma digital** el proceso de verificación regresa un valor verdadero si y sólo si se satisfacen las siguientes dos condiciones:

- 1 Autenticidad del signatario
- 2 Autenticidad del documento



Problemas matemáticos computacionalmente difíciles

- Problema de factorización entera: Dado un entero $N = p \cdot q$ encuentre sus factores primos p y q . Por ejemplo: ¿Cuál es la factorización de 2018?

Problemas matemáticos computacionalmente difíciles

- Problema de factorización entera: Dado un entero $N = p \cdot q$ encuentre sus factores primos p y q . Por ejemplo: ¿Cuál es la factorización de 2018?

Respuesta: $2018 = 2 \cdot 1009$

Problemas matemáticos computacionalmente difíciles

- Problema de factorización entera: Dado un entero $N = p \cdot q$ encuentre sus factores primos p y q . Por ejemplo: ¿Cuál es la factorización de 2018?
Respuesta: $2018 = 2 \cdot 1009$
- Problema del logaritmo discreto: Dado un número primo p y $g, h \in [1, p - 1]$, encuentre un entero x (en caso de que exista) tal que: $g^x \equiv h \pmod{p}$.
Por ejemplo: ¿Cuánto vale x tal que: $2^x \equiv 304 \pmod{419}$?

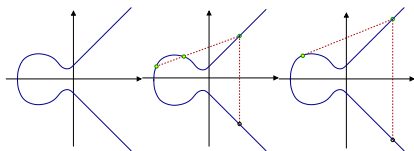
Problemas matemáticos computacionalmente difíciles

- Problema de factorización entera: Dado un entero $N = p \cdot q$ encuentre sus factores primos p y q . Por ejemplo: ¿Cuál es la factorización de 2018?
Respuesta: $2018 = 2 \cdot 1009$
- Problema del logaritmo discreto: Dado un número primo p y $g, h \in [1, p - 1]$, encuentre un entero x (en caso de que exista) tal que: $g^x \equiv h \pmod{p}$.
Por ejemplo: ¿Cuánto vale x tal que: $2^x \equiv 304 \pmod{419}$?
Respuesta: $2^{343} \equiv 304 \pmod{419}$.

Problemas matemáticos computacionalmente difíciles

- Problema de factorización entera: Dado un entero $N = p \cdot q$ encuentre sus factores primos p y q . Por ejemplo: ¿Cuál es la factorización de 2018?
Respuesta: $2018 = 2 \cdot 1009$
- Problema del logaritmo discreto: Dado un número primo p y $g, h \in [1, p - 1]$, encuentre un entero x (en caso de que exista) tal que: $g^x \equiv h \pmod{p}$.
Por ejemplo: ¿Cuánto vale x tal que: $2^x \equiv 304 \pmod{419}$?
Respuesta: $2^{343} \equiv 304 \pmod{419}$.
- Problema del logaritmo discreto para curvas elípticas: Dada una curva elíptica definida sobre E/\mathbb{F}_q y $P, Q \in E(\mathbb{F}_{q^k})$, encuentre un entero x (en caso de que exista) tal que: $xP = Q$

Firma digital ECDSA

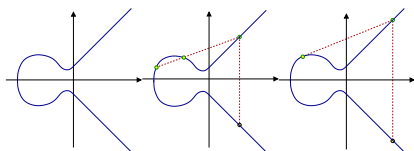


Una curva elíptica está definida por el conjunto de puntos afines $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, donde p es un primo impar grande, que satisface la ecuación corta de Weierstrass,

$$E : y^2 = x^3 + ax + b,$$

junto con un punto al infinito denotado por \mathcal{O} . El conjunto de puntos que satisfacen la anterior ecuación forman un grupo abeliano denotado por $E(\mathbb{F}_p)$ con orden $\#E(\mathbb{F}_p) = h \cdot r$, donde r es un primo grande y el cofactor h es un entero pequeño.

Firma digital ECDSA



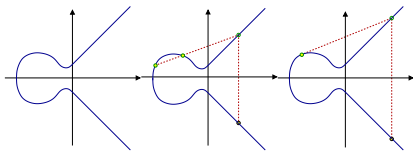
Una curva elíptica está definida por el conjunto de puntos afines $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, donde p es un primo impar grande, que satisface la ecuación corta de Weierstrass,

$$E : y^2 = x^3 + ax + b,$$

junto con un punto al infinito denotado por \mathcal{O} . El conjunto de puntos que satisfacen la anterior ecuación forman un grupo abeliano denotado por $E(\mathbb{F}_p)$ con orden $\#E(\mathbb{F}_p) = h \cdot r$, donde r es un primo grande y el cofactor h es un entero pequeño.



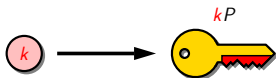
Firma digital ECDSA



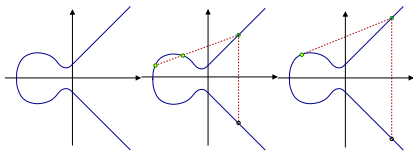
Una curva elíptica está definida por el conjunto de puntos afines $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, donde p es un primo impar grande, que satisface la ecuación corta de Weierstrass,

$$E : y^2 = x^3 + ax + b,$$

junto con un punto al infinito denotado por \mathcal{O} . El conjunto de puntos que satisfacen la anterior ecuación forman un grupo abeliano denotado por $E(\mathbb{F}_p)$ con orden $\#E(\mathbb{F}_p) = h \cdot r$, donde r es un primo grande y el cofactor h es un entero pequeño.



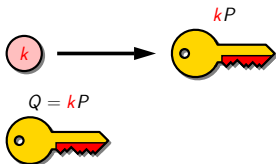
Firma digital ECDSA



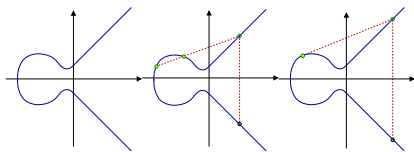
Una curva elíptica está definida por el conjunto de puntos afines $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, donde p es un primo impar grande, que satisface la ecuación corta de Weierstrass,

$$E : y^2 = x^3 + ax + b,$$

junto con un punto al infinito denotado por \mathcal{O} . El conjunto de puntos que satisfacen la anterior ecuación forman un grupo abeliano denotado por $E(\mathbb{F}_p)$ con orden $\#E(\mathbb{F}_p) = h \cdot r$, donde r es un primo grande y el cofactor h es un entero pequeño.



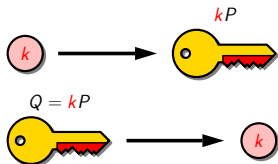
Firma digital ECDSA



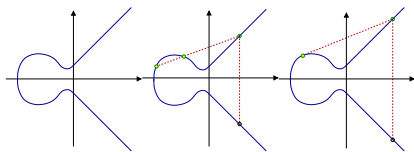
Una curva elíptica está definida por el conjunto de puntos afines $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, donde p es un primo impar grande, que satisface la ecuación corta de Weierstrass,

$$E : y^2 = x^3 + ax + b,$$

junto con un punto al infinito denotado por \mathcal{O} . El conjunto de puntos que satisfacen la anterior ecuación forman un grupo abeliano denotado por $E(\mathbb{F}_p)$ con orden $\#E(\mathbb{F}_p) = h \cdot r$, donde r es un primo grande y el cofactor h es un entero pequeño.



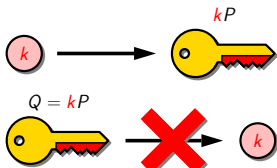
Firma digital ECDSA



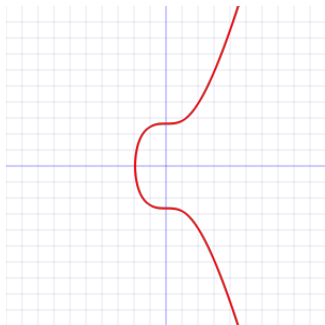
Una curva elíptica está definida por el conjunto de puntos afines $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$, donde p es un primo impar grande, que satisface la ecuación corta de Weierstrass,

$$E : y^2 = x^3 + ax + b,$$

junto con un punto al infinito denotado por \mathcal{O} . El conjunto de puntos que satisfacen la anterior ecuación forman un grupo abeliano denotado por $E(\mathbb{F}_p)$ con orden $\#E(\mathbb{F}_p) = h \cdot r$, donde r es un primo grande y el cofactor h es un entero pequeño.

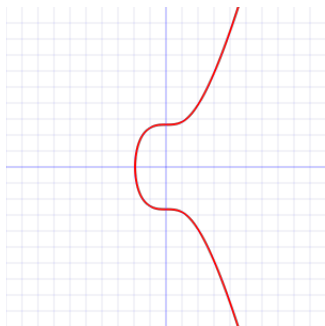


Secp256k1: La curva elíptica escogida por Satoshi Nakamoto



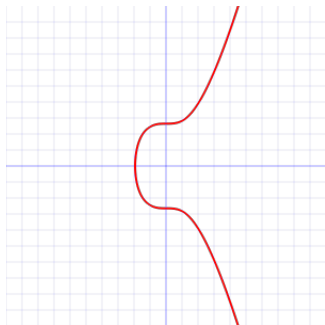
- La curva elíptica utilizada en Bitcoin se conoce como la curva de Koblitz [Secp256k1](#)

Secp256k1: La curva elíptica escogida por Satoshi Nakamoto



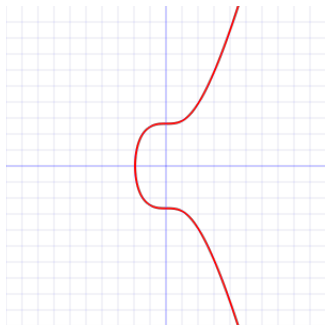
- Se considera que la capacidad de cómputo de todo el planeta tierra no puede vulnerar un esquema con una seguridad superior a 2^{90} operaciones en un tiempo razonable (digamos menos de un siglo)

Secp256k1: La curva elíptica escogida por Satoshi Nakamoto



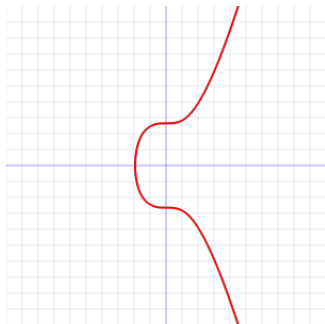
- Secp256k1 ofrece una seguridad estimada de 2^{128} operaciones, por lo que actualmente se considera invulnerable

Secp256k1: La curva elíptica escogida por Satoshi Nakamoto



- Una llave secreta típica de Bitcoin es un número de 256 bits que puede escribirse con unos 78 dígitos decimales

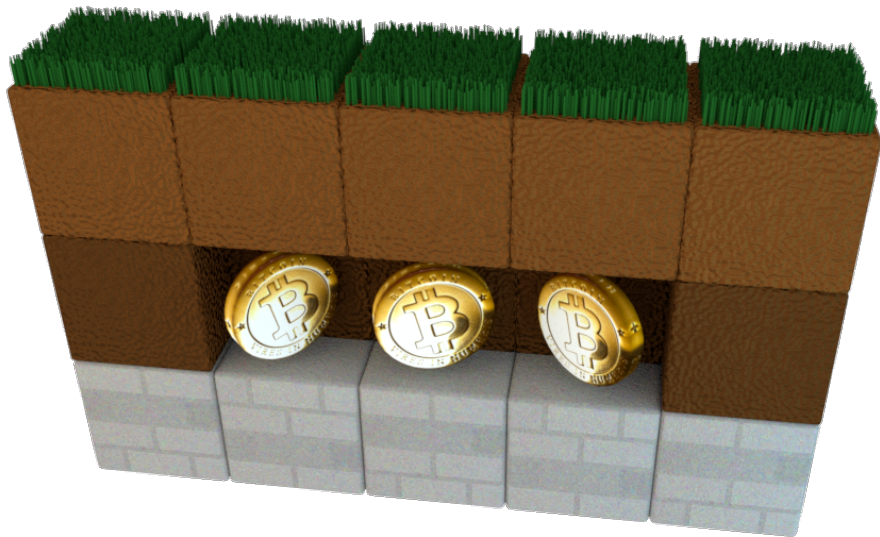
Secp256k1: La curva elíptica escogida por Satoshi Nakamoto



- **Ejemplo de una llave secreta de Bitcoin:**

50055567251691925235369028159807142878767134421137157309464273410328506669646

Bloques básicos del sistema Bitcoin



La bitácora de bloques blockchain

- En la **blockchain** se encuentran almacenadas de forma ordenada y con marcas de tiempo, todas las transacciones realizadas desde que se acuñó el bloque génesis en enero de 2009
- La **blockchain** previene el problema del **doble gasto** y modificaciones en las transacciones ya realizadas
- Cada cliente de la red Bitcoin puede almacenar de forma independiente una copia de la **blockchain**, y verificar cada una de sus transacciones
- Cuando varios nodos de la red tienen en su **blockchain** los mismos bloques se dice que los nodos están en consenso
- Para enero de 2018, la bitácora de Bitcoin alcanzó un tamaño de unos 151 Gigabytes

Billeteras (Wallets)

- Permite generar pares de llaves públicas/privadas
- Crea las direcciones de depósito (derivados a partir de los picadillos de las llaves públicas)
- Verifica si se han realizado transacciones hacia las direcciones administradas
- Crea y firma transacciones desde las direcciones administradas
- Comunica a la red Bitcoin las transacciones que ya hayan sido firmadas
- Existen billeteras de software y de hardware

¿Se debe adquirir una billetera para guardar bitcoins?

Existen tres opciones para comprar/vender **cripto-monedas**:

- Adquirir una cuenta con usuario/contraseña en una casa de cambio (**broker**)

[A pesar de la opinión de Bart, esta sería la opción más simple y por lo tanto es recomendable para usuarios primerizos y/o con inversiones pequeñas]



¿Se debe adquirir una billetera para guardar bitcoins?

Existen tres opciones para comprar/vender **cripto-monedas**:

- Billetera de software

[Esta opción es gratuita. Sin embargo la seguridad de las llaves privadas depende del usuario, por lo que se recomienda utilizar un dispositivo digital (laptop, tableta, computadora) que se conecte muy rara vez a Internet]



Bitcoin
Knots



Bitcoin
Core



Bither



Electrum



Green
Address



ArcBit



mSIGNA



Armory

¿Se debe adquirir una billetera para guardar bitcoins?

Existen tres opciones para comprar/vender **cripto-monedas**:

- Billetera de hardware

[Es la opción más segura, pero no es gratuita. Los usuarios avanzados o con inversiones fuertes deberían adquirir una]



Acuñaación de bitcoins

- Las primeras monedas de bitcoins fueron creadas por Satoshi Nakamoto el 3 de enero del 2009 (mediante una transacción de 50 BTC)
- Esta acción fue realizada a favor de una entidad representada por la llave pública de Nakamoto (y sin que a nadie se le hubiera cargado esa cantidad de dinero)
- Esta transacción constituye el primer bloque, el cual fue llamado el **bloque génesis**

Acuñaación de bitcoins: Mineros

- La organización de los bloques generados posteriormente al bloque génesis y los cálculos para confirmarlos, son llevados a cabo por los mineros
- Cuando un minero forma un bloque, la primera transacción que coloca en el bloque (conocida como la transacción base), es una transacción especial que le da al minero una recompensa de 25 BTC, lo cual debe sumarse a las “propinas” correspondientes a todas las otras transacciones incluidas en ese bloque.
- La recompensa de 25 BTC se otorgará al minero sólo si su bloque es confirmado por la red Bitcoin.
- Este mecanismo es el único existente en Bitcoin para acuñar nuevas monedas. Sólo se generarán 21 millones de Bitcoins

2

²M. en C. Abraham Jesús Basurto Becerra, “Aspectos de seguridad de Bitcoin y su aplicación en una alternativa de infraestructura de llave pública”, 17 de diciembre de 2015, Director de Tesis: Dr. Francisco Rodríguez Henríquez.

Acuñaación de bitcoins: Los mineros y sus granjas



Bitcoin: Protocolo de compra-venta

Supongamos que Alicia quiere comprar un taco al pastor en la taquería de Beto. Para realizar la compra-venta Alicia y Beto siguen el siguiente procedimiento:

Bitcoin: Protocolo de compra-venta

Supongamos que Alicia quiere comprar un taco al pastor en la taquería de Beto. Para realizar la compra-venta Alicia y Beto siguen el siguiente procedimiento:

- 1 Tanto Beto como Alicia deben tener instalado una aplicación conocida como **wallet** que actúa como una billetera digital

Bitcoin: Protocolo de compra-venta

Supongamos que Alicia quiere comprar un taco al pastor en la taquería de Beto. Para realizar la compra-venta Alicia y Beto siguen el siguiente procedimiento:

- 1 Tanto Beto como Alicia deben tener instalado una aplicación conocida como **wallet** que actúa como una billetera digital
- 2 Las billeteras pueden generar y administrar direcciones electrónicas. Cada dirección tiene asociada un determinado saldo de bitcoins así como una pareja de llave pública/privada

Bitcoin: Protocolo de compra-venta

Supongamos que Alicia quiere comprar un taco al pastor en la taquería de Beto. Para realizar la compra-venta Alicia y Beto siguen el siguiente procedimiento:

- 1 Tanto Beto como Alicia deben tener instalado una aplicación conocida como **wallet** que actúa como una billetera digital
- 2 Las billeteras pueden generar y administrar direcciones electrónicas. Cada dirección tiene asociada un determinado saldo de bitcoins así como una pareja de llave pública/privada
- 3 Para vender su producto, la billetera de Beto crea una nueva dirección para que Alicia le envíe su pago (las direcciones se derivan a partir de los picadillos de las llaves públicas)

Bitcoin: Protocolo de compra-venta

Supongamos que Alicia quiere comprar un taco al pastor en la taquería de Beto. Para realizar la compra-venta Alicia y Beto siguen el siguiente procedimiento:


- 1 Tanto Beto como Alicia deben tener instalado una aplicación conocida como **wallet** que actúa como una billetera digital
- 2 Las billeteras pueden generar y administrar direcciones electrónicas. Cada dirección tiene asociada un determinado saldo de bitcoins así como una pareja de llave pública/privada
- 3 Para vender su producto, la billetera de Beto crea una nueva dirección para que Alicia le envíe su pago (las direcciones se derivan a partir de los picadillos de las llaves públicas)
- 4 Alicia firma su solicitud de transacción con su clave privada indicando que transferirá ese dinero a la dirección indicada por Beto

Bitcoin: Protocolo de compra-venta

Supongamos que Alicia quiere comprar un taco al pastor en la taquería de Beto. Para realizar la compra-venta Alicia y Beto siguen el siguiente procedimiento:

- 1 Tanto Beto como Alicia deben tener instalado una aplicación conocida como **wallet** que actúa como una billetera digital
- 2 Las billeteras pueden generar y administrar direcciones electrónicas. Cada dirección tiene asociada un determinado saldo de bitcoins así como una pareja de llave pública/privada
- 3 Para vender su producto, la billetera de Beto crea una nueva dirección para que Alicia le envíe su pago (las direcciones se derivan a partir de los picadillos de las llaves públicas)
- 4 Alicia firma su solicitud de transacción con su clave privada indicando que transferirá ese dinero a la dirección indicada por Beto
- 5 A partir de ese momento, cualquier miembro de la red Bitcoin puede verificar la transacción que hizo Alicia usando la llave pública que corresponda

Recibiendo/Enviando bitcoins


1 BTC = 189498.74 MXN | Wallet

FONDEAR - BITCOIN

Manda Bitcoin a la siguiente dirección para fondear tu cuenta Bitso.

37p6cog73ocAaUzyW4zqsDh4fjoMsd9qHE

Wallet Name: **chavosebuap88.bitso.io**



Recibiendo/Enviando bitcoins



1 BTC = 189481.41 MXN ▼

Wallet

Exchange ▼

Ayuda



RETIRAR - BITCOIN

Para retirar Bitcoin de tu saldo Bitso, favor complete el siguiente formulario:

Saldo: **0.00000000 BTC**

Una comisión de **aproximadamente 0.00049236 BTC** será agregada al monto enviado. Esto es **aproximadamente 92 MXN**. ?

Monto

BTC

[Máximo]

Dirección

NIP de Transacción ?

Enviar

Recibiendo/Enviando bitcoins: Cajeros ATM



Distribución de riqueza de Bitcoin [fuente: bitinfocharts.com]

Bitcoin distribution					
Balance	Addresses	% Addresses (Total)	Coins	\$USD	% Coins (Total)
0 - 0.001	15213311	53.62% (100%)	2,797 BTC	38,880,873 USD	0.02% (100%)
0.001 - 0.01	5966376	21.03% (46.38%)	25,875 BTC	359,704,754 USD	0.15% (99.98%)
0.01 - 0.1	4667190	16.45% (25.36%)	150,274 BTC	2,089,088,037 USD	0.9% (99.83%)
0.1 - 1	1829078	6.45% (8.91%)	570,118 BTC	7,925,703,956 USD	3.4% (98.93%)
1 - 10	549335	1.94% (2.46%)	1,460,657 BTC	20,305,836,215 USD	8.7% (95.54%)
10 - 100	131714	0.46% (0.53%)	4,362,397 BTC	60,645,406,889 USD	25.99% (86.83%)
100 - 1,000	15711	0.06% (0.06%)	3,707,665 BTC	51,543,423,365 USD	22.09% (60.84%)
1,000 - 10,000	1517	0.01% (0.01%)	3,330,041 BTC	46,293,749,977 USD	19.84% (38.75%)
10,000 - 100,000	109	0% (0%)	2,733,655 BTC	38,002,877,799 USD	16.29% (18.9%)
100,000 - 1,000,000	3	0% (0%)	438,618 BTC	6,097,610,026 USD	2.61% (2.61%)

Addresses richer than

1 USD	100 USD	1,000 USD	10,000 USD	100,000 USD	1,000,000 USD	10,000,000 USD
21,803,815	8,457,461	2,955,222	846,066	178,589	22,380	2,239

[Bitcoin UTXOs cumulative chart](#)

Multi-millonarios en dólares [fuente: Wikipedia]

No. ↕	Name ↕	Net worth (USD) ↕	Age ↕	Nationality ↕	Source(s) of wealth ↕
1 —	Bill Gates	\$86.0 billion ▲	61	 United States	Microsoft
2 ▲	Warren Buffett	\$75.6 billion ▲	86	 United States	Berkshire Hathaway
3 ▲	Jeff Bezos	\$72.8 billion ▲	53	 United States	Amazon.com
4 ▼	Amancio Ortega	\$71.3 billion ▲	80	 Spain	Inditex, Zara
5 ▲	Mark Zuckerberg	\$56.0 billion ▲	32	 United States	Facebook
6 ▼	Carlos Slim	\$54.5 billion ▲	77	 Mexico	América Móvil, Grupo Carso
7 —	Larry Ellison	\$52.2 billion ▲	72	 United States	Oracle Corporation
8 ▲	Charles Koch	\$48.3 billion ▲	81	 United States	Koch Industries
8 ▲	David Koch	\$48.3 billion ▲	76	 United States	Koch Industries
10 ▼	Michael Bloomberg	\$47.5 billion ▲	75	 United States	Bloomberg L.P.

Multi-millonarios en bitcoins [fuente: bitinfocharts.com]

	Address	Balance Δ_{1w}	% of coins	First In	Last In	Number Of Ins Δ_{1w}	First Out	Last Out	Number Of Outs Δ_{1w}
1	16rCmCmbuWDhPjWTrpQGaU3EPdZF7MTdUk	179,203 BTC (\$2,491,254,438 USD) <small>+0.00006 BTC</small>	1.07%	2016-02-27 12:00:09	2018-01-13 20:29:12	91 <small>-1</small>	2016-11-16 14:50:07	2017-10-27 15:25:49	32
2	3D2oetdNuZuQqHPJmcMDDHYoqkyNVsFk9r <small>wallet: Bitfinex-coldwallet</small>	142,245 BTC (\$1,977,474,714 USD) <small>-3699 BTC</small>	0.8472%	2017-01-05 06:34:15	2018-01-14 16:09:13	4144 <small>-58</small>	2017-01-06 04:29:06	2018-01-14 15:04:03	3789 <small>-75</small>
3	16ftSEQ4ctQFDtVZIUBusQUJrRghM3JYwe	117,170 BTC (\$1,628,880,873 USD) <small>-26369 BTC</small>	0.6978%	2017-12-08 01:51:10	2018-01-13 20:29:12	81 <small>-6</small>	2017-12-10 10:55:29	2018-01-07 21:24:45	39
4	1FeexV6bAHb8ybZjqQMjrcCrHGw9sb6uF	79,957 BTC (\$1,111,553,004 USD)	0.4762%	2011-03-01 04:26:19	2017-12-25 17:36:04	118			
5	3Nxwenay9Z8Lc9JBiywExpnEFilp6Afp8v	78,348 BTC (\$1,089,187,173 USD)	0.4666%	2015-10-16 09:43:06	2017-12-23 12:59:13	152	2015-10-29 04:44:26	2017-12-29 07:21:16	51
6	18rnfQgGo1HqvVQaAN4QnxjYE7Sez9eca <small>wallet: 29043297</small>	69,600 BTC (\$967,569,186 USD)	0.4145%	2014-10-24 05:40:08	2017-12-17 03:00:08	251	2014-10-27 00:55:11	2018-01-06 12:12:34	101
7	1HQ3Go3ggs8pFnXuHVHRYtPCq5fGG8Hbhx	69,370 BTC (\$964,373,242 USD)	0.4132%	2013-04-09 16:03:36	2017-12-14 21:48:03	82	2015-04-23 09:10:25	2015-04-23 09:10:25	1
8	1PhMfRF2enSZnR6JSexxBHuxQnxG8Vo5FVK	66,452 BTC (\$923,807,077 USD)	0.3958%	2013-11-22 13:06:31	2017-12-09 01:47:57	125			
9	1AhTjUMztCihTyA4K6E3QEpojWLwKhkR	66,379 BTC (\$922,788,563 USD)	0.3953%	2014-02-24 23:33:06	2017-12-30 23:12:49	192			
10	1DIHQMPFu4p84rLn6Majj2LCZZZRQUaa	66,236 BTC (\$920,800,805 USD)	0.3945%	2013-11-22 18:08:37	2017-12-28 21:20:37	138			

Multi-millonarios en bitcoins [fuente: bitinfocharts.com]

	Address	Balance $\Delta 1w$	% of coins	First In	Last In	Number Of Ins $\Delta 1w$	First Out	Last Out	Number Of Outs $\Delta 1w$
1	16rCmCmbuWDhPJwTrpQGau3EPdZF7MTdUk	179,203 BTC (\$2,491,254,438 USD) <small>+0.00006 BTC</small>	1.07%	2016-02-27 12:00:09	2018-01-13 20:29:12	91 $\Delta 1$	2016-11-16 14:50:07	2017-10-27 15:25:49	32
2	3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r wallet: Bitfinex-coldwallet	142,245 BTC (\$1,977,474,714 USD) <small>-3699 BTC</small>	0.8472%	2017-01-05 06:34:15	2018-01-14 16:09:13	4144 $\Delta 58$	2017-01-06 04:29:06	2018-01-14 15:04:03	3789 $\Delta 75$
3	16ftSEQ4ctQFDtVziUBusQUjRrGhM3JYwe	117,170 BTC (\$1,628,880,873 USD) <small>-26369 BTC</small>	0.6978%	2017-12-08 01:51:10	2018-01-13 20:29:12	81 $\Delta 6$	2017-12-10 10:55:29	2018-01-07 21:24:45	39
4	1FeexV6bAHb8ybZjqQMjJrcCrHGw9sb6uF	79,957 BTC (\$1,111,553,004 USD)	0.4762%	2011-03-01 04:26:19	2017-12-25 17:36:04	118			
5	3Nxwenay9Z8Lc9JBiywExprEFilp6Afp8v	78,348 BTC (\$1,089,187,173 USD)	0.4666%	2015-10-16 09:43:06	2017-12-23 12:59:13	152	2015-10-29 04:44:26	2017-12-29 07:21:16	51
6	18mfoQgGo1HqvVQaAN4QnxjYE7Sez9eca wallet: 29043297	69,600 BTC (\$967,569,186 USD)	0.4145%	2014-10-24 05:40:08	2017-12-17 03:00:08	251	2014-10-27 00:55:11	2018-01-06 12:12:34	101
7	1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx	69,370 BTC (\$964,373,242 USD)	0.4132%	2013-04-09 16:03:36	2017-12-14 21:48:03	82	2015-04-23 09:10:25	2015-04-23 09:10:25	1
8	1PnMIRF2enSZnR6JSexxBHuQnxG8Vo5FVK	66,452 BTC (\$923,807,077 USD)	0.3958%	2013-11-22 13:06:31	2017-12-09 01:47:57	125			
9	1AhTjUmZtCihITyA4K6E3QEpojWlWKhkR	66,379 BTC (\$922,788,563 USD)	0.3953%	2014-02-24 23:33:06	2017-12-30 23:12:49	192			
10	1DIHDQMPFu4p84rkLn6Majj2LCZZRQUaa	66,236 BTC (\$920,800,805 USD)	0.3945%	2013-11-22 18:08:37	2017-12-28 21:20:37	138			

La persona/entidad en el mundo con más bitcoins es el propio Satoshi Nakamoto.

Multi-millonarios en bitcoins [fuente: bitinfocharts.com]

Address	Balance Δ_{1w}	% of coins	First In	Last In	Number Of Ins Δ_{1w}	First Out	Last Out	Number Of Outs Δ_{1w}
1 16rCmCmbuWDhPjWTrpQGaU3EPdZF7MTdUk	179,203 BTC (\$2,491,254,438 USD) <small>+0.00006 BTC</small>	1.07%	2016-02-27 12:00:09	2018-01-13 20:29:12	91 <small>-1</small>	2016-11-16 14:50:07	2017-10-27 15:25:49	32
2 3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r <small>wallet: Bitfinex-coldwallet</small>	142,245 BTC (\$1,977,474,714 USD) <small>-3699 BTC</small>	0.8472%	2017-01-05 06:34:15	2018-01-14 16:09:13	4144 <small>-58</small>	2017-01-06 04:29:06	2018-01-14 15:04:03	3789 <small>-75</small>
3 16ftSEQ4ctQFDtVZIUBusQUjRrGhM3JYwe	117,170 BTC (\$1,628,880,873 USD) <small>+26369 BTC</small>	0.6978%	2017-12-08 01:51:10	2018-01-13 20:29:12	81 <small>-6</small>	2017-12-10 10:55:29	2018-01-07 21:24:45	39
4 1FeexV6bAHb8ybZjqQMjJrcCrHGw9sb6uF	79,957 BTC (\$1,111,553,004 USD)	0.4762%	2011-03-01 04:26:19	2017-12-25 17:36:04	118			
5 3Nxwenay9Z8Lc9JBiywExpnEFilp6Aip8v	78,348 BTC (\$1,089,187,173 USD)	0.4666%	2015-10-16 09:43:06	2017-12-23 12:59:13	152	2015-10-29 04:44:26	2017-12-29 07:21:16	51
6 18mfoQgGo1HqvVQaAN4QnxjYE7Sez9eca <small>wallet: 29043297</small>	69,600 BTC (\$967,569,186 USD)	0.4145%	2014-10-24 05:40:08	2017-12-17 03:00:08	251	2014-10-27 00:55:11	2018-01-06 12:12:34	101
7 1HQ3Go3ggs8pFnXuHVHRytPCq5iGG8Hbhx	69,370 BTC (\$964,373,242 USD)	0.4132%	2013-04-09 16:03:36	2017-12-14 21:48:03	82	2015-04-23 09:10:25	2015-04-23 09:10:25	1
8 1PnMfRF2enSZnR6JSexxBHuQnxG8Vo5FVK	66,452 BTC (\$923,807,077 USD)	0.3958%	2013-11-22 13:06:31	2017-12-09 01:47:57	125			
9 1AhTjUMztCihITyA4K6E3QEpojWlwKtkR	66,379 BTC (\$922,788,563 USD)	0.3953%	2014-02-24 23:33:06	2017-12-30 23:12:49	192			
10 1DIHDQMPFu4p84rkLn6Majj2LCZZRZQOua	66,236 BTC (\$920,800,805 USD)	0.3945%	2013-11-22 18:08:37	2017-12-28 21:20:37	138			

Dado que durante los primeros diez días, Nakamoto se reservó el derecho de exclusivo de minado de monedas, se estima que su fortuna alcanza un millón de bitcoins [de un total de 21 millones de monedas que Nakamoto estipuló que se crearan]

Satoshi Nakamoto: ¿Cuál es la verdadera identidad del misterioso genio multi-millonario?



La verdad en el caso del temible pirata Roberts



La verdad en el caso del temible pirata Roberts



Por primera vez en la historia del planeta, una persona fue condenada a cadena perpetua por crímenes cometidos detrás de una computadora

La verdad en el caso del temible pirata Roberts



Se trata del estadounidense Ross Ulbricht, quien tenía 29 años cuando fue capturado por el FBI en octubre de 2013. Su nombre de guerra en la red era el del “**Dread Pirate Roberts**”

La verdad en el caso del temible pirata Roberts



El FBI descubrió que Ulbricht es el fundador del sitio de Internet conocido como “[Silk Road](#)”, de un modelo económico similar a lo que entre nosotros sería “[Mercado libre](#)”, pero con un giro diferente, pues en [Silk Road](#), se vendían todo tipo de drogas, venenos, animales pertenecientes a especies en peligro de extinción, y se podían contratar a sicarios y asesinos a sueldo.

La verdad en el caso del temible pirata Roberts



En 2013 el reconocido criptógrafo Adi Shamir especuló sobre los posibles nexos entre el pirata Roberts y Satoshi Nakamoto. Sin embargo retiró su comentario poco después

La verdad en el caso del temible pirata Roberts



En el sitio “[Silk Road](#)” se trasegaron unos nueve millones de Bitcoins durante sus aproximadamente dos años y 8 meses de existencia [[de febrero de 2011 a octubre de 2013](#)]



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	-	Creación del bloque génesis



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	-	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	-	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"
11.febrero.2012	4.3	se anuncian regulaciones en contra de BTC



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"
11.febrero.2012	4.3	se anuncian regulaciones en contra de BTC
11.marzo.2013	68.9	ocurre un "hard fork" de Bitcoin versión 0.8



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	-	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"
11.febrero.2012	4.3	se anuncian regulaciones en contra de BTC
11.marzo.2013	68.9	ocurre un "hard fork" de Bitcoin versión 0.8
1.octubre.2013	135.1	el FBI aprehende al temible pirata Roberts



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"
11.febrero.2012	4.3	se anuncian regulaciones en contra de BTC
11.marzo.2013	68.9	ocurre un "hard fork" de Bitcoin versión 0.8
1.octubre.2013	135.1	el FBI aprehende al temible pirata Roberts
18.noviembre.2013	1,072.2	BTC rompe por primera vez la barrera de 1000 USD



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"
11.febrero.2012	4.3	se anuncian regulaciones en contra de BTC
11.marzo.2013	68.9	ocurre un "hard fork" de Bitcoin versión 0.8
1.octubre.2013	135.1	el FBI aprehende al temible pirata Roberts
18.noviembre.2013	1,072.2	BTC rompe por primera vez la barrera de 1000 USD
7.febrero.2014	626.5	Ataques de denegación de servicio a las principales casas de bolsa



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"
11.febrero.2012	4.3	se anuncian regulaciones en contra de BTC
11.marzo.2013	68.9	ocurre un "hard fork" de Bitcoin versión 0.8
1.octubre.2013	135.1	el FBI aprehende al temible pirata Roberts
18.noviembre.2013	1,072.2	BTC rompe por primera vez la barrera de 1000 USD
7.febrero.2014	626.5	Ataques de denegación de servicio a las principales casas de bolsa
10.abril.2014	408.5	China anuncia fuertes restricciones a BTC



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"
11.febrero.2012	4.3	se anuncian regulaciones en contra de BTC
11.marzo.2013	68.9	ocurre un "hard fork" de Bitcoin versión 0.8
1.octubre.2013	135.1	el FBI aprehende al temible pirata Roberts
18.noviembre.2013	1,072.2	BTC rompe por primera vez la barrera de 1000 USD
7.febrero.2014	626.5	Ataques de denegación de servicio a las principales casas de bolsa
10.abril.2014	408.5	China anuncia fuertes restricciones a BTC
13.junio.2014	592.3	Una granja minera alcanza el 51% de las decisiones en la Blockchain



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"
11.febrero.2012	4.3	se anuncian regulaciones en contra de BTC
11.marzo.2013	68.9	ocurre un "hard fork" de Bitcoin versión 0.8
1.octubre.2013	135.1	el FBI aprehende al temible pirata Roberts
18.noviembre.2013	1,072.2	BTC rompe por primera vez la barrera de 1000 USD
7.febrero.2014	626.5	Ataques de denegación de servicio a las principales casas de bolsa
10.abril.2014	408.5	China anuncia fuertes restricciones a BTC
13.junio.2014	592.3	Una granja minera alcanza el 51% de las decisiones en la Blockchain
11.diciembre.2014	324.9	Microsoft anuncia que aceptará BTC



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"
11.febrero.2012	4.3	se anuncian regulaciones en contra de BTC
11.marzo.2013	68.9	ocurre un "hard fork" de Bitcoin versión 0.8
1.octubre.2013	135.1	el FBI aprehende al temible pirata Roberts
18.noviembre.2013	1,072.2	BTC rompe por primera vez la barrera de 1000 USD
7.febrero.2014	626.5	Ataques de denegación de servicio a las principales casas de bolsa
10.abril.2014	408.5	China anuncia fuertes restricciones a BTC
13.junio.2014	592.3	Una granja minera alcanza el 51% de las decisiones en la Blockchain
11.diciembre.2014	324.9	Microsoft anuncia que aceptará BTC
19.mayo.2015	238.2	El temible pirata Roberts es condenado a dos cadenas perpetuas



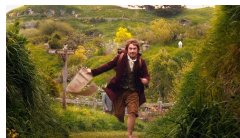
Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"
11.febrero.2012	4.3	se anuncian regulaciones en contra de BTC
11.marzo.2013	68.9	ocurre un "hard fork" de Bitcoin versión 0.8
1.octubre.2013	135.1	el FBI aprehende al temible pirata Roberts
18.noviembre.2013	1,072.2	BTC rompe por primera vez la barrera de 1000 USD
7.febrero.2014	626.5	Ataques de denegación de servicio a las principales casas de bolsa
10.abril.2014	408.5	China anuncia fuertes restricciones a BTC
13.junio.2014	592.3	Una granja minera alcanza el 51% de las decisiones en la Blockchain
11.diciembre.2014	324.9	Microsoft anuncia que aceptará BTC
19.mayo.2015	238.2	El temible pirata Roberts es condenado a dos cadenas perpetuas
8.diciembre.2015	461.1	La revista Wired anuncia que el empresario australiano Craig Wright es Satoshi Nakamoto



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"
11.febrero.2012	4.3	se anuncian regulaciones en contra de BTC
11.marzo.2013	68.9	ocurre un "hard fork" de Bitcoin versión 0.8
1.octubre.2013	135.1	el FBI aprehende al temible pirata Roberts
18.noviembre.2013	1,072.2	BTC rompe por primera vez la barrera de 1000 USD
7.febrero.2014	626.5	Ataques de denegación de servicio a las principales casas de bolsa
10.abril.2014	408.5	China anuncia fuertes restricciones a BTC
13.junio.2014	592.3	Una granja minera alcanza el 51% de las decisiones en la Blockchain
11.diciembre.2014	324.9	Microsoft anuncia que aceptará BTC
19.mayo.2015	238.2	El temible pirata Roberts es condenado a dos cadenas perpetuas
8.diciembre.2015	461.1	La revista Wired anuncia que el empresario australiano Craig Wright es Satoshi Nakamoto
21.febrero.2016	433.7	Se crean las bases para ampliar el tamaño del bloque en BTC



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"
11.febrero.2012	4.3	se anuncian regulaciones en contra de BTC
11.marzo.2013	68.9	ocurre un "hard fork" de Bitcoin versión 0.8
1.octubre.2013	135.1	el FBI aprehende al temible pirata Roberts
18.noviembre.2013	1,072.2	BTC rompe por primera vez la barrera de 1000 USD
7.febrero.2014	626.5	Ataques de denegación de servicio a las principales casas de bolsa
10.abril.2014	408.5	China anuncia fuertes restricciones a BTC
13.junio.2014	592.3	Una granja minera alcanza el 51% de las decisiones en la Blockchain
11.diciembre.2014	324.9	Microsoft anuncia que aceptará BTC
19.mayo.2015	238.2	El temible pirata Roberts es condenado a dos cadenas perpetuas
8.diciembre.2015	461.1	La revista Wired anuncia que el empresario australiano Craig Wright es Satoshi Nakamoto
21.febrero.2016	433.7	Se crean las bases para ampliar el tamaño del bloque en BTC
3.enero.2017	1,020.5	BTC rompe después de 3 años la barrera de 1000 USD



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"
11.febrero.2012	4.3	se anuncian regulaciones en contra de BTC
11.marzo.2013	68.9	ocurre un "hard fork" de Bitcoin versión 0.8
1.octubre.2013	135.1	el FBI aprehende al temible pirata Roberts
18.noviembre.2013	1,072.2	BTC rompe por primera vez la barrera de 1000 USD
7.febrero.2014	626.5	Ataques de denegación de servicio a las principales casas de bolsa
10.abril.2014	408.5	China anuncia fuertes restricciones a BTC
13.junio.2014	592.3	Una granja minera alcanza el 51% de las decisiones en la Blockchain
11.diciembre.2014	324.9	Microsoft anuncia que aceptará BTC
19.mayo.2015	238.2	El temible pirata Roberts es condenado a dos cadenas perpetuas
8.diciembre.2015	461.1	La revista Wired anuncia que el empresario australiano Craig Wright es Satoshi Nakamoto
21.febrero.2016	433.7	Se crean las bases para ampliar el tamaño del bloque en BTC
3.enero.2017	1,020.5	BTC rompe después de 3 años la barrera de 1000 USD
1.abril.2017	1,215.7	Japón declara a BTC como una moneda de validez legal en ese país



Bitcoin: Un viaje inesperado



Fecha	Precio (en USD)	Observaciones
3.enero.2009	–	Creación del bloque génesis
5.octubre.2009	0.00076	Primera casa de cambio
22.mayo.2010	10,000 BTC por 2 pizzas	Primera compra de algo usando BTC
11.julio.2010	0.08	Se lanza la versión 0.3 de BTC
9.febrero.2011	1.00	por primera vez BTC rompe la barrera de 1 USD
1.junio.2011	17.6	se publica por primera vez noticias sobre la "silk road"
19.diciembre.2011	4.2	aparece BTC en un capítulo de la "Good Wife"
11.febrero.2012	4.3	se anuncian regulaciones en contra de BTC
11.marzo.2013	68.9	ocurre un "hard fork" de Bitcoin versión 0.8
1.octubre.2013	135.1	el FBI aprehende al temible pirata Roberts
18.noviembre.2013	1,072.2	BTC rompe por primera vez la barrera de 1000 USD
7.febrero.2014	626.5	Ataques de denegación de servicio a las principales casas de bolsa
10.abril.2014	408.5	China anuncia fuertes restricciones a BTC
13.junio.2014	592.3	Una granja minera alcanza el 51% de las decisiones en la Blockchain
11.diciembre.2014	324.9	Microsoft anuncia que aceptará BTC
19.mayo.2015	238.2	El temible pirata Roberts es condenado a dos cadenas perpetuas
8.diciembre.2015	461.1	La revista Wired anuncia que el empresario australiano Craig Wright es Satoshi Nakamoto
21.febrero.2016	433.7	Se crean las bases para ampliar el tamaño del bloque en BTC
3.enero.2017	1,020.5	BTC rompe después de 3 años la barrera de 1000 USD
1.abril.2017	1,215.7	Japón declara a BTC como una moneda de validez legal en ese país
1.agosto.2017	3,383.8	Se crea Bitcoin cash (BCH)

El Bitcoin y otras bestias fantásticas



Bestiario de criptomonedas

Top 100 Cryptocurrencies described in 4 words or less

by @eigenjoy

Updated November 7th, 2017

1 - 33		
1	Bitcoin	BTC Digital gold
2	Ethereum	ETH Programmable contracts and money
3	Bitcoin Cash	BCH Bitcoin clone
4	Ripple	XRP Enterprise payment settlement network
5	Litecoin	LTC Faster Bitcoin
6	Dash	DASH Privacy-focused Bitcoin clone
7	NEO	NEO Chinese-market Ethereum
8	NEM	XEM Batteries-included digital assets
9	Monero	XMR Private digital cash
10	Ethereum Classic	ETC Ethereum clone
11	IOTA	MIOTA Internet-of-things payments
12	Qtum	QTUM Ethereum contracts on Bitcoin
13	OmiseGO	OMG Banking, remittance, and exchange
14	Zcash	ZEC Private digital cash
15	BitConnect	BCC Madoff-like investment fund
16	Lisk	LSK Decentralized applications in JavaScript
17	Cardano	ADA Layered currency and contracts
18	Tether	USDt Price = 1 USD
19	Stellar Lumens	XLM Digital IOUs
20	EOS	EOS Decentralized applications on WebAssembly
21	Hshare	HSR Blockchain switchboard
22	Waves	WAVES Decentralized exchange and crowdfunding
23	Stratis	STRAT Decentralized applications in C#
24	Komodo	KMD Decentralized ICOs
25	Ark	ARK Blockchain switchboard
26	Electroneum	ETN Monero clone
27	Bytecoin	BCN Privacy-focused cryptocurrency
28	Stem	STEM Reddit with money voting
29	Ardr	ARDR Blockchain for spawning blockchains
30	Binance Coin	BNB Pay Binance exchange fees
31	Augur	REP Decentralized prediction market
32	Populous	PPT Invoice trading futures
33	Decred	DCR Bitcoin with alternative governance

34 - 66		
34	TenX	PAY Cryptocurrency credit card
35	MaidSafeCoin	MAID Rent disk space
36	BitcoinDark	BTCd Zcoin clone
37	BitShares	BTS Decentralized exchange
38	Golem	GNT Rent other people's computers
39	PIVX	PIVX Inflationary Dash clone
40	Gas	GAS Pay fees on Neo
41	TRON	TRX In-app-purchases
42	Vertcoin	VTC Bitcoin clone
43	MonaCoin	MONA Japanese Dogecoin
44	Factom	FCT Decentralized record keeping
45	Basic Attention Token	BAT Decentralized ad network
46	SALT	SALT Cryptocurrency-backed loans
47	Kyber Network	KNC Decentralized exchange
48	Dogecoin	DOGE Serious meme bitcoin clone
49	DigixDAO	DGD Organisation manages tokenized gold
50	Veritaseum	VERI Vaporware
51	Walton	WTC IoT Blockchain
52	SingularDTV	SNGLS Decentralized Netflix
53	Bytom	BTM Physical assets as tokens
54	Byteball Bytes	GBYTE Decentralized database and currency
55	GameCredits	GAME Video game currency
56	Metaverse ETP	ETP Chinese Ethereum plus identity
57	GXShares	GXS Decentralized Chinese Equifax
58	Sysoin	SYS Decentralized marketplace
59	Siacoin	SC Rent disk space
60	Status	SNT Decentralized application browser
61	Ox	ORX Decentralized exchange
62	Verge	XVG Privacy Dogecoin
63	Lykke	LKR Digital asset exchange
64	Civic	CVC Identity and Authentication App
65	Blocknet	BLOCK Decentralized exchange
66	Metal	MTL Payments with rewards program

67 - 100		
67	Iconomi	ICN Digital asset investment funds
68	Aeternity	AE Decentralized apps (prototype)
69	DigiByte	DBG Faster Bitcoin
70	Bancor	BNT Token Index Funds
71	Ripio Credit Net	RCN Co-signed Cryptocurrency Loans
72	ATMChain	ATM Advertising network
73	Gnosis	GNO Decentralized prediction market
74	VeChain	VEN Supply chain item IDs
75	Pura	PURA Cryptocurrency
76	Particl	PART Privacy marketplace and chat
77	KuCoin Shares	KCS Profit-sharing exchange fees
78	Bitquize	BQX Mint for cryptocurrency investments
79	FunFair	FUN Decentralized casino
80	ChainLink	LINK External data for contracts
81	Power Ledger	POWR AirbnB for electricity
82	Nxt	NXT Cryptocurrency and marketplace
83	Monaco	MCO Cryptocurrency credit card
84	Cryptonex	CNX Zerocoin clone
85	MCAP	HCAP Mining investment fund
86	Storj	STORJ Rent disk space
87	ZenCash	ZEN Privacy-focused Bitcoin clone
88	Nexus	NXS Bitcoin clone
89	Neblio	NEBL Decentralized application platform
90	Zeusshield	ZSC Decentralized insurance
91	Streamr DATA	DATA Real-time data marketplace
92	ZCoin	ZXC Private digital cash
93	NAV Coin	NAV Bitcoin with private transactions
94	AdEx	ADX Advertising exchange
95	Open Trading Ne	OTN Decentralized exchange
96	SmartCash	SMART Zcoin clone with rewards
97	Bitdel	BDL Bitcoin clone
98	Loopring	LRC Decentralized exchange
99	Edgeless	EDG Decentralized casino
100	FairCoin	FAIR Bitcoin that rewards savers













Learn to program smart contracts and cryptocurrency
<https://newline.co>

Ranked according to market cap on coinmarketcap.com as of November 7th, 2017











Caution: market cap is not an indicator of maturity or legitimacy

10 criptomonedas principales [a 15 de enero de 2018]











All ▾ Coins ▾ Tokens ▾

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)
1	 Bitcoin	BTC	\$228,617,257,385	\$13,605.70	16,803,050	\$10,940,600,000
2	 Ethereum	ETH	\$129,320,441,348	\$1,333.44	96,982,572	\$4,767,020,000
3	 Ripple	XRP	\$71,139,399,684	\$1.84	38,739,142,811 *	\$1,920,350,000
4	 Bitcoin Cash	BCH	\$42,931,037,731	\$2,538.52	16,911,838	\$986,439,000
5	 Cardano	ADA	\$20,112,224,939	\$0.775723	25,927,070,538 *	\$150,889,000
6	 Litecoin	LTC	\$13,081,529,846	\$238.90	54,758,033	\$972,155,000
7	 NEM	XEM	\$12,276,359,999	\$1.36	8,999,999,999 *	\$37,805,300
8	 Stellar	XLM	\$11,096,504,988	\$0.620246	17,890,490,206 *	\$112,776,000
9	 NEO	NEO	\$10,338,120,000	\$159.05	65,000,000 *	\$533,550,000
10	 IOTA	MIOTA	\$10,291,655,598	\$3.70	2,779,530,283 *	\$132,923,000

10 criptomonedas principales [a 1 de febrero de 2018]

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)
1	 Bitcoin	BTC	\$172,437,165,158	\$10,240.90	16,838,087	\$7,308,840,000
2	 Ethereum	ETH	\$112,550,974,050	\$1,156.29	97,338,016	\$3,707,170,000
3	 Ripple	XRP	\$44,524,446,398	\$1.15	38,739,142,811 *	\$781,873,000
4	 Bitcoin Cash	BCH	\$25,143,880,712	\$1,484.02	16,943,088	\$661,890,000
5	 Cardano	ADA	\$13,381,920,406	\$0.516137	25,927,070,538 *	\$335,719,000
6	 Stellar	XLM	\$9,833,586,263	\$0.533569	18,429,830,563 *	\$241,564,000
7	 NEO	NEO	\$9,353,305,000	\$143.90	65,000,000 *	\$267,305,000
8	 Litecoin	LTC	\$9,010,478,040	\$163.78	55,014,733	\$294,931,000
9	 NEM	XEM	\$7,119,593,999	\$0.791066	8,999,999,999 *	\$48,260,500
10	 IOTA	MIOTA	\$6,357,869,774	\$2.29	2,779,530,283 *	\$44,817,000

10 criptomonedas principales [a 7 de febrero de 2018]

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)
1	 Bitcoin	BTC	\$125,711,384,734	\$7,460.29	16,850,737	\$12,224,300,000
2	 Ethereum	ETH	\$73,499,275,539	\$754.14	97,460,791	\$5,561,280,000
3	 Ripple	XRP	\$28,537,425,902	\$0.731556	39,009,215,838 *	\$2,059,950,000
4	 Bitcoin Cash	BCH	\$15,770,395,204	\$930.20	16,953,750	\$640,328,000
5	 Cardano	ADA	\$8,917,356,641	\$0.343940	25,927,070,538 *	\$1,190,120,000
6	 Litecoin	LTC	\$7,674,955,441	\$139.28	55,106,483	\$970,985,000
7	 NEO	NEO	\$6,607,315,000	\$101.65	65,000,000 *	\$657,364,000
8	 Stellar	XLM	\$6,427,903,515	\$0.348734	18,432,110,190 *	\$439,427,000
9	 NEM	XEM	\$5,258,690,999	\$0.584299	8,999,999,999 *	\$64,396,200
10	 EOS	EOS	\$5,119,329,315	\$7.84	653,338,181 *	\$1,172,250,000

Algunas Características de la criptomoneda Ethereum

- Inició operaciones en julio del 2015
- Se dice que la bitácora de bloques de Ethereum es "Turing complete" lo cual permite programar contratos para diversas aplicaciones
- El tiempo para validar un bloque en la bitacora de Ethereum es menor a 15 segundos [lo cual es mucho más rápido que los 10 minutos de Bitcoin]
- Algunas de las aplicaciones actuales de Ethereum incluyen: pagos en video juegos, firmas digitales con validez legal, apuestas en línea, fondeos, etc.
- Es la segunda cripto-moneda por capitalización de mercado inmediatamente después de Bitcoin

Algunas Características de la criptomoneda **Ripple**

- **Ripple** inició operaciones en agosto de 2012
- **Ripple** se define como un sistema de intercambio y crédito. El MIT es una de las entidades que validan esta cripto moneda
- **Ripple** puede pensarse como una alternativa a sistemas de pago tipo **paypal** pero en el caso de **Ripple** no existe una autoridad central.
- Por criterio de diseño en **Ripple** no existen **mineros** pues su número de monedas ha sido fijado en 200 mil millones, de los cuales 39 mil millones están en circulación. El resto es retenido por los diseñadores y por la red **Ripple**
- Es la tercera cripto-moneda por capitalización de mercado inmediatamente después de **Bitcoin** y **Ethereum**

Capitalización de mercado [fuente: marketwatch.com]



" Gold. Gold beyond measure, beyond sorrow, and grief "

Thorin Oakenshield, son of Thráin, son of Thrór, King under the Mountain

Escenarios [súper] optimistas para diciembre de 2018

- La capitalización de mercado de **Bitcoin** alcanza el medio billón de dólares [en español] aumentado su valor actual tres veces

Escenarios [súper] optimistas para diciembre de 2018

- La capitalización de mercado de **Bitcoin** alcanza el medio billón de dólares [en español] aumentado su valor actual tres veces
- La capitalización de mercado de **Etherum** alcanza 300 billones de dólares [en español] aumentado su valor actual unas cuatro veces

Escenarios [súper] optimistas para diciembre de 2018

- La capitalización de mercado de **Bitcoin** alcanza el medio billón de dólares [en español] aumentado su valor actual tres veces
- La capitalización de mercado de **Etherum** alcanza 300 billones de dólares [en español] aumentado su valor actual unas cuatro veces
- Surge una nueva cripto-moneda cuya capitalización de mercado desbanca a **ripple** en el tercer lugar de las cripto-monedas por mercado de capitalización

Escenarios pesimistas para diciembre de 2018

- Moderadamente pesimistas:

Escenarios pesimistas para diciembre de 2018

- **Moderadamente pesimistas:**
 - ▶ Regulaciones agresivas de los principales países consumidores de la tecnología Bitcoin [en el Japón se comercia la mitad de bitcoins en el mundo] estabilizan el crecimiento de las cripto-monedas para que observen una conducta similar al dinero tradicional
- **Altamente pesimistas:**

Escenarios pesimistas para diciembre de 2018

- **Moderadamente pesimistas:**
 - ▶ Regulaciones agresivas de los principales países consumidores de la tecnología Bitcoin [en el Japón se comercia la mitad de bitcoins en el mundo] estabilizan el crecimiento de las cripto-monedas para que observen una conducta similar al dinero tradicional
- **Altamente pesimistas:**
 - ▶ El valor de la gran mayoría de cripto-monedas desciende drásticamente debido a las presiones del mundo financiero y/o a la venta masiva de monedas por los multi-millonarios [conocidos en la jerga como **Ballenas**]

Escenarios pesimistas para diciembre de 2018

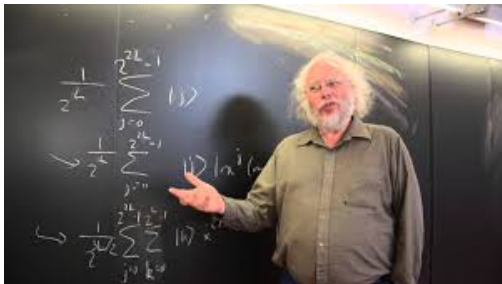
- **Moderadamente pesimistas:**

- ▶ Regulaciones agresivas de los principales países consumidores de la tecnología Bitcoin [en el Japón se comercia la mitad de bitcoins en el mundo] estabilizan el crecimiento de las cripto-monedas para que observen una conducta similar al dinero tradicional

- **Altamente pesimistas:**

- ▶ El valor de la gran mayoría de cripto-monedas desciende drásticamente debido a las presiones del mundo financiero y/o a la venta masiva de monedas por los multi-millonarios [conocidos en la jerga como **Ballenas**] y/o a la venta por parte de Satoshi Nakamoto de una parte importante de su fortuna.

Escenarios [Apocalípticos] para diciembre de 2018



Una implementación cuántica del algoritmo de Peter Shor para factorización de números enteros hace que el esfuerzo computacional para romper la curva [Secp256k1](#) de Bitcoin se reduzca de **miles de millones de años** a **cientos de horas**.

Escenarios [Apocalípticos] para diciembre de 2018

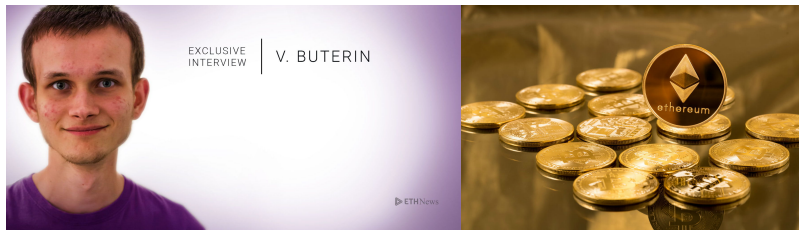


Junto con Bitcoin perecen la enorme mayoría de criptomonedas

Escenarios [Apocalípticos] para diciembre de 2018

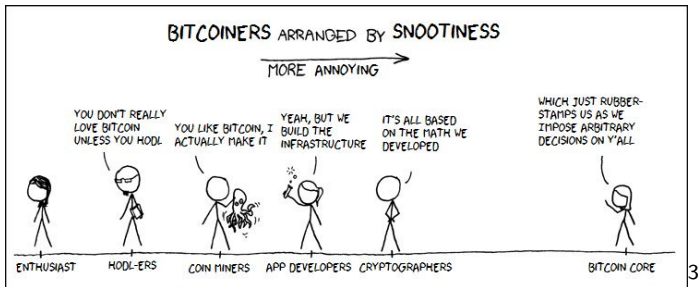
- Posibles bestias sobrevivientes: Ethereum, IOTA, Quantum Resistant Ledger, ...

Pronóstico



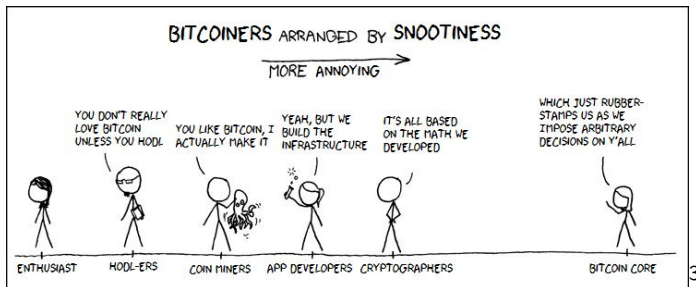
- Ethereum se consolida como la cripto-moneda con mayor capitalización de mercado

Proyectos de investigación



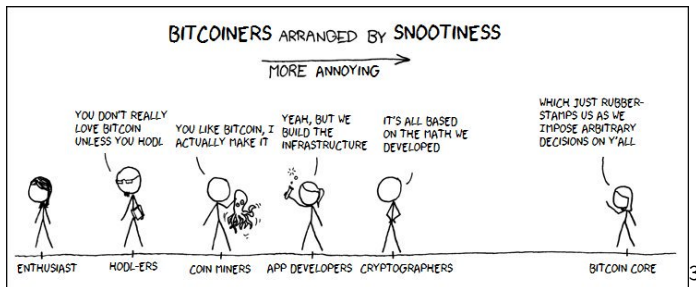
Proy0 : Utilizar la **Blockchain** de la cripto-moneda **Ethereum** para revolucionar los contratos de diversas industrias tales como: agricultura, video-juegos, fotografía, campañas políticas, notarías digitales, juegos de loterías incorruptibles...

Proyectos de investigación



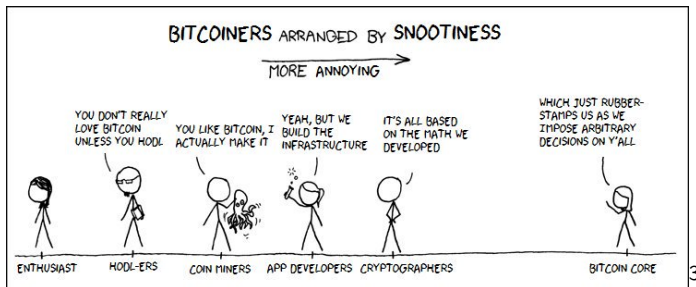
Proy1 : Extender el trabajo realizado en la tesis de maestría:
M. en C. Abraham Jesús Basurto Becerra, "Aspectos de seguridad de Bitcoin y su aplicación en una alternativa de infraestructura de llave pública", 17 de diciembre de 2015, Director de Tesis: Dr. Francisco Rodríguez Henríquez.

Proyectos de investigación



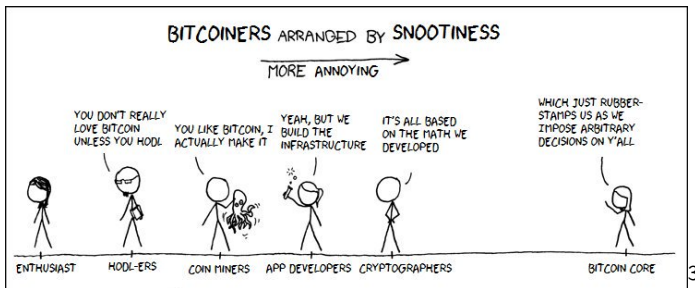
Proy2 : Convertirse en **minero** para **ciertas** cripto-monedas (especialmente atractivo resulta **Litecoin** y más recientemente **Petro**) utilizando GPUs, procesadores multi-núcleo y/o hardware personalizado

Proyectos de investigación



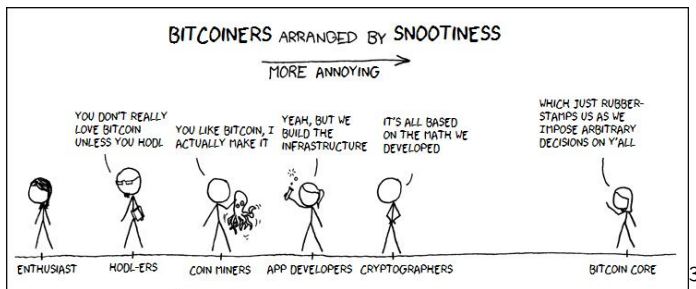
Proy3 : Utilizando la gran información estadística disponible públicamente, predecir mediante **inteligencia artificial** el comportamiento de las principales crypto-monedas

Proyectos de investigación



Proy4 : Yin-Yang 

Proyectos de investigación

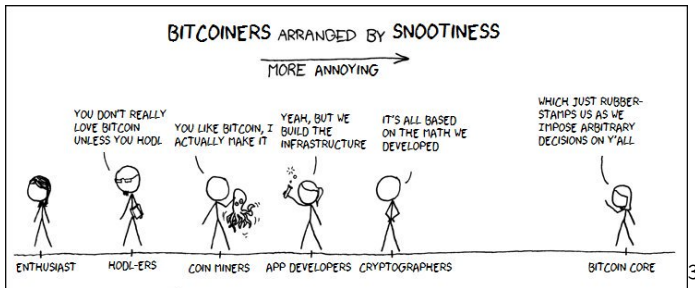


Proy4 : Yin-Yang 

4Yin: Construir una **computadora cuántica** capaz de ejecutar el algoritmo de Shor y con ello destruir al 99.9% del ecosistema de criptomonedas

³cómic cortesía de **XKCD**

Proyectos de investigación



Proy4 : Yin-Yang ☯

4Yin: Construir una **computadora cuántica** capaz de ejecutar el algoritmo de Shor y con ello destruir al 99.9% del ecosistema de criptomonedas

4Yang: Crear una criptomoneda que sea resistente al cómputo cuántico

³cómic cortesía de **XKCD**

Gracias



- Mis sinceros agradecimientos al Dr. Andrés Cortés Dávalos por el diseño de las animaciones que hermocean esta presentación
- Agradezco los valiosos comentarios críticos sobre el material técnico presentado aquí vertidos por la Dra. Nareli Cruz Cortés, el Dr. Luis Julián Domínguez Pérez y el Maestro Adrián Ramírez Cabrera
- Agradezco a los niños Ana Iremi y Andrés Enrique Rodríguez Cruz por sus creativas sugerencias para ilustrar de mejor manera el material de esta presentación y definir su título
- Agradezco el súper entusiasta apoyo de los doctorantes Carlos, Huguet, Karina, Pao y Sandra del Departamento de Bioquímica