

Bitcoin, blockchain y otras palabrejas



Programa

- Qué es el bitcoin, de dónde viene, a dónde va
- Blockchain y elementos relacionados
- Investigando transacciones en bitcoins y otras criptomonedas
- ~~Oportunidades de negocio, o cómo hacerse rico con bitcoins~~

¿Cuánto vale un bitcoin y por qué?

- A 24 de abril de 2024, a las 14:04

1 BTC = 62.275 €



Agosto 2022: 12,6 M USD



Abril 2022: 522.000 USD

Qué es bitcoin

- Criptomoneda: un bien digital basado en criptografía para su generación, intercambio y contabilidad.
- Aparece en 2009, tras un “paper” firmado por “Satoshi Nakamoto”
- Se forma un grupo de desarrollo descentralizado

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the

Qué es bitcoin

- La primera y principal criptomoneda. Primera realización de dinero electrónico descentralizado e independiente. Un sueño ciberpunk.
- Basada en:
 - Descentralización: Red P2P de nodos
 - Escasez (suministro limitado): 21M BTC
 - Anonimato y Pseudoanonimato
 - Transparencia: Todas las transacciones son públicas
 - Matemáticas para dar seguridad: Cifrado y hash
 - Consenso y minería con PoW: generación y registro
 - Blockchain: libro de contabilidad de los bitcoins

Uso del bitcoin

- Pagos P2P
- Pagos B2B
- Pagos anónimos
- Especulación

60.425,35 EUR

+ Seguir

+60.118,33 (19.581,22 %) ↑ desde siempre

24 abr, 16:02 UTC · [Renuncia de responsabilidad](#)

1 D

5 D

1 M

6 M

YTD

1 A

5 A

Máx.

80.000

60.000

40.000

20.000

0

2019

2022

59.866,83 15 mar 2024

24 abril a las 18:02
4 horas más tarde que
hace 4 transparencias



Uso del bitcoin

- 18 mayo 2010
- Laszlo Hanyecz dijo que pagaría 10.000 bitcoins por un par de pizzas grandes
- Jeremy Sturdivant le envió dos pizzas de Papa John's, le costaron 25 USD. Laszlo pagó (al cambio, 41 USD).
- Primera transacción de algo físico por bitcoins.

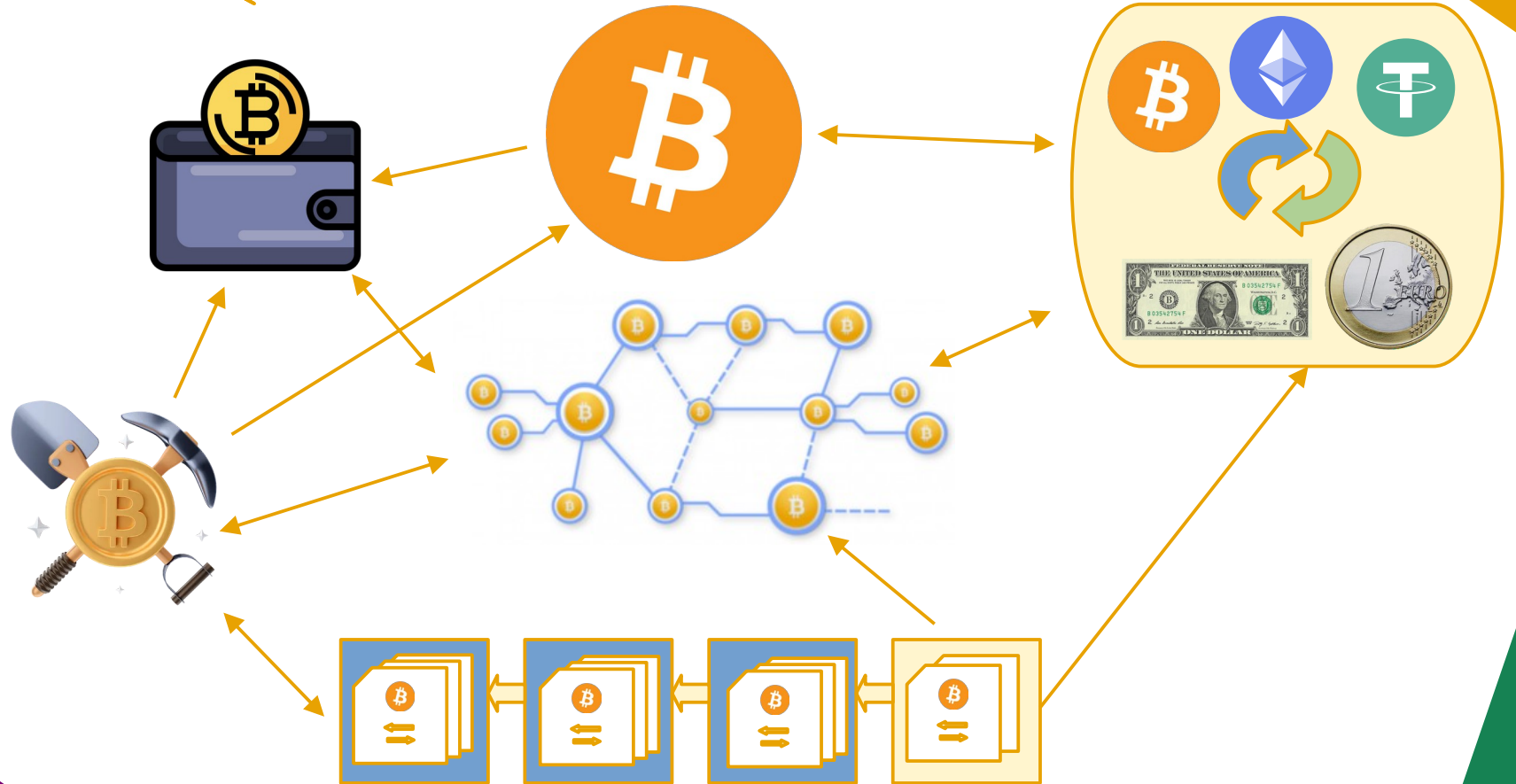


<https://bitcoinpizzaindex.net/>

De dónde vienen los bitcoins

- “Satoshi” desaparece en 2011, una vez formado el ecosistema, y no ha vuelto a aparecer. No hay pistas de su identidad (aunque sí sospechas).
- Se ha llamado “satoshi” a la menor fracción de bitcoin que se puede hacer ($1/100.000.000$)
- Se “crean” como “*premio*” a los *mineros*. El minero que “gane” anota X bitcoins en su *cartera*. Ahora mismo (desde el **20 de abril 2024**) 3,125 BTC.

Conceptos clave

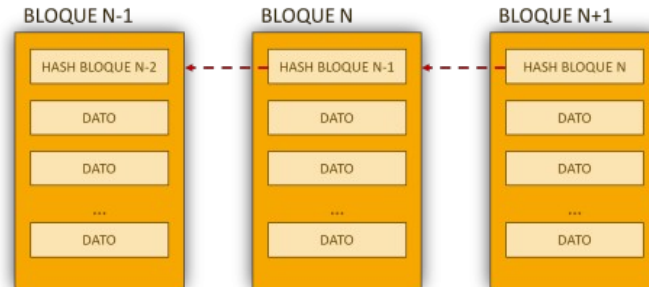


Qué es una cartera de bitcoins

- Los bitcoins se “guardan” en carteras virtuales.
- Programas que generan y almacenan claves privadas usadas para generar *direcciones* de bitcoins
- Generan y firman *transacciones* de bitcoins y las envían a red
- Descarga una copia del *blockchain* para saber qué fondos hay en cada dirección.
- NO guarda físicamente bitcoins, sólo las claves privadas y direcciones generadas. El contenido es cosa del blockchain

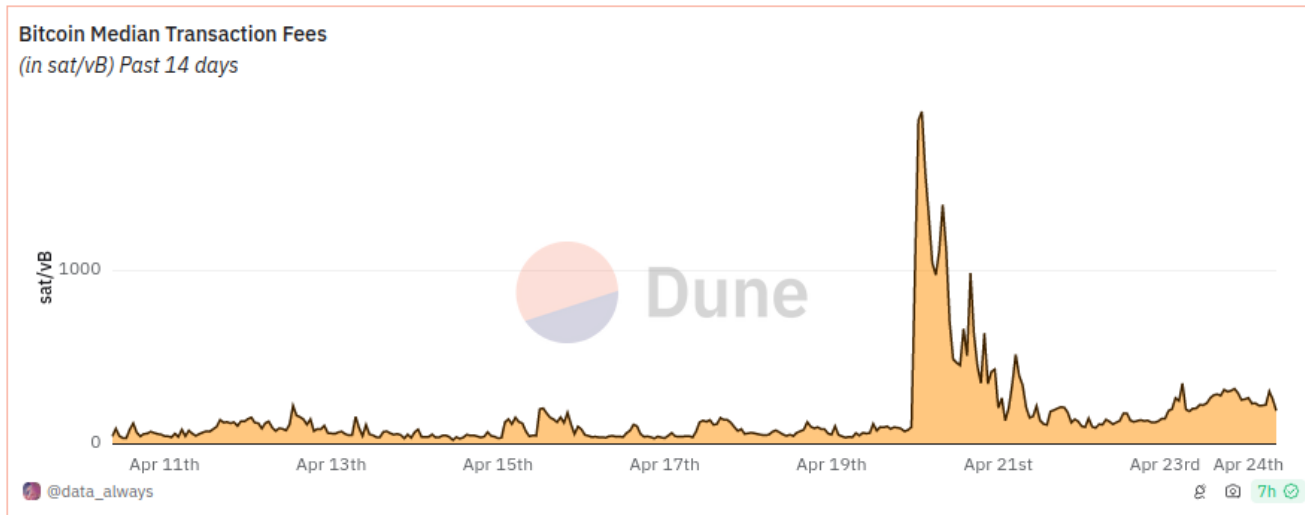
Blockchain: libro “mayor” de contabilidad de bitcoins

- Almacena todas las transacciones: desde la generación de bitcoins hasta cada gasto.
- Sólo el minero “ganador” puede añadir *bloques* (AKA páginas del libro), y sólo tras el *consenso* del 51% de la red.
- Cada bloque hace referencia al anterior, quedando “encadenado”. Se transmite a toda la red.



Bloque

- Tamaño limitado (máximo 4MB, típico 1,5MB): espacio es recurso limitado
- Firmado y encadenado con el bloque anterior
- Hay que “pagar” por el espacio que ocupa tu transacción, y es un precio variable



OJO

- Cada movimiento de bitcoin es rastreable, desde el inicio de los tiempos. Se sabe cuándo aparecen y dónde se anotan, cuándo se mueven y a qué número de cartera.
- La red no permite gastar bitcoins que no tienes



Consenso

- Bitcoin requiere consenso. Las normas, algoritmos y validaciones son comunes y aceptados por todos.
- Todo el código está publicado como software libre.
- Todos los nodos tienen las mismas reglas y validan todos los mensajes siguiendo las mismas normas.
- Cualquier cambio (BIP) pasa por un proceso de discusión público y debe ser aceptado por el 51% de la comunidad **como poco.**

Minería de bitcoins

- Resolver un problema muy complicado, para el que no hay algoritmos eficientes.
- Encontrar la solución requiere ensayo y error.
- Probabilidad muy baja
- Consumo de energía alto
- Hoy por hoy: procesadores de diseño específico (ASICs)



Minería de bitcoins

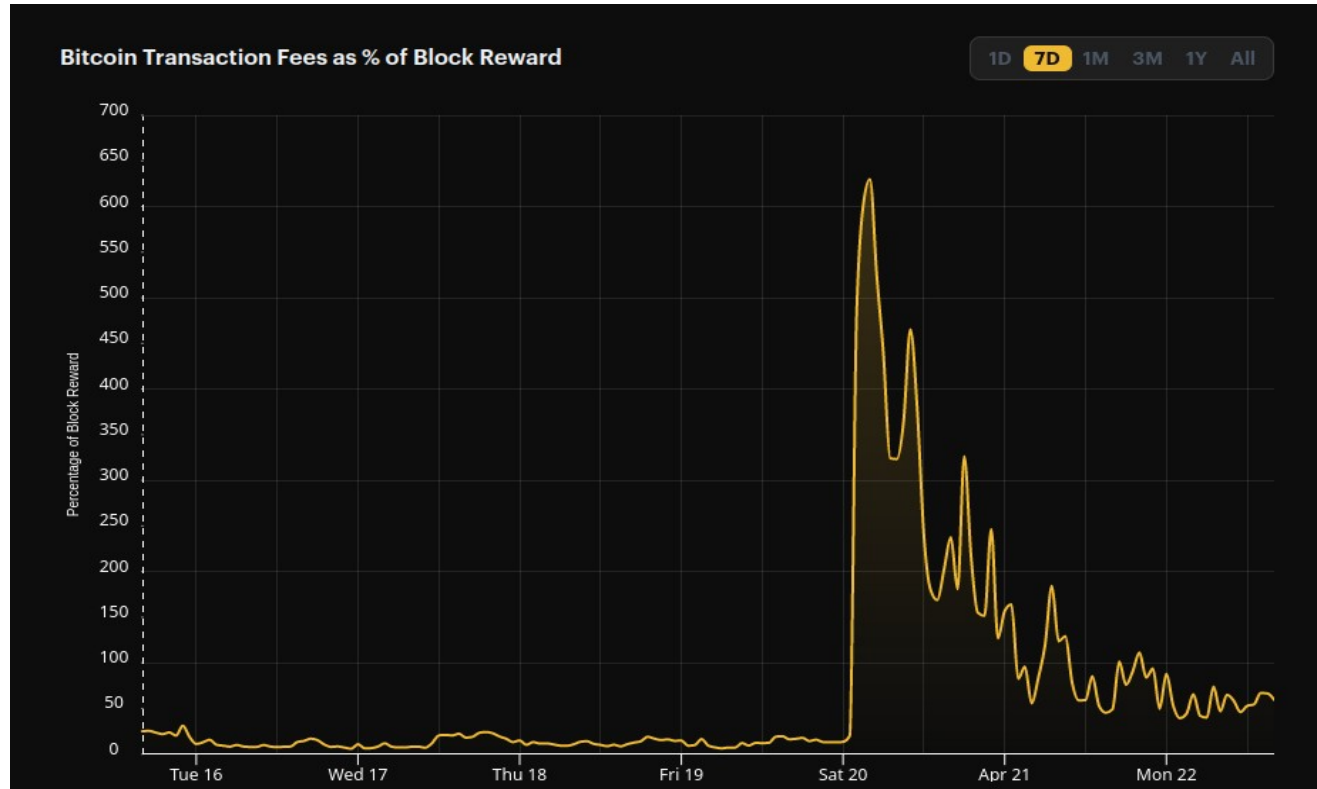


Lanza el dado y que salga un número menor que 4

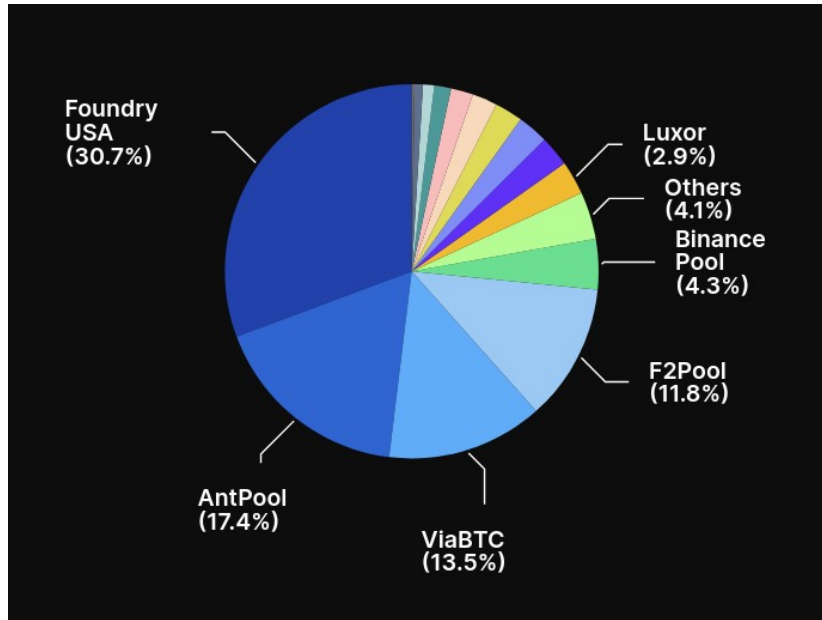
Minería de bitcoins

- PoW: *Proof of Work* → Encontrar un número que, puesto a continuación de una cadena, genera un *hash* menor que X.
- La dificultad depende de X → fijado por la red
- No hay fórmula para hallarlo a priori. Hay que calcular el hash con todas las opciones → Resultado al azar.
- Incentivo para mineros:
 - Premio (ahora mismo 3,125 BTC)
 - *Tarifas* por anotar transacciones (15-80% premio)
- Organización en “*pools*” de mineros que trabajan coordinados.

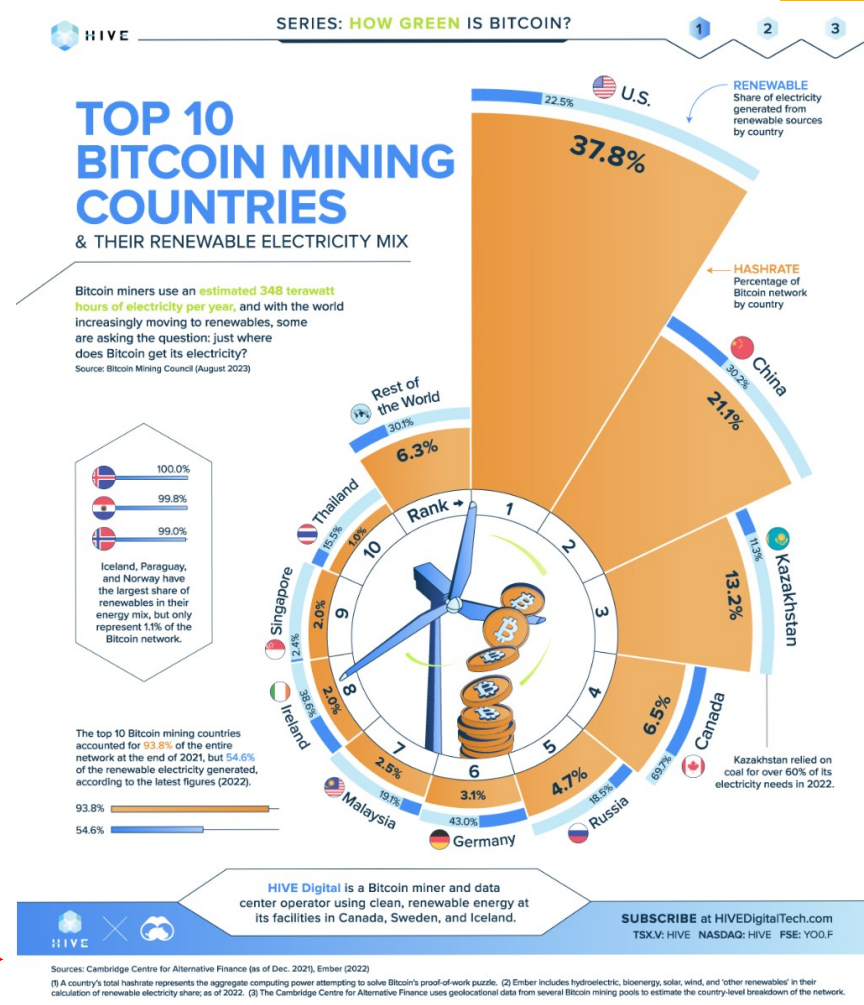
Minería de bitcoins



Minería de bitcoins



China prohibió el minado de bitcoins en 2021



Minería de bitcoins

- Las transacciones son anotadas en los bloques por el último minero ganador. Cobra precios de procesado.
- En la red de bitcoin, en media, cada 10 minutos se genera un nuevo bloque (nueva solución).
- Para mantener el ritmo, se ajusta la dificultad cada 2 semanas aprox (2016 bloques).
- A 22 abril 2024: unos 650 ExaHash/s ($650 \cdot 10^{18}$)

650 ExaHash/s

650.000.000.000.000.000.000

lanzamientos de dado cada segundo

y hacen falta aproximadamente 600 seg
para encontrar una solución

Hashrate de la red de bitcoin

Total Hash Rate (TH/s)

The estimated number of terahashes per second the bitcoin network is performing in the last 24 hours.

Scales

Linear

Average

Type

Line

Colors



1M

3M

6M

1Y

3Y

All



Características económicas

- Como moneda: no hay autoridad que respalde el valor. Depende únicamente de mercado.
- No hay una autoridad responsable del funcionamiento: depende del consenso.
- Diseñada para ser inflacionista. Sólo 21 millones de BTC.
- Transmisible sin control: al introducir la transacción en la red y anotarse, queda hecha, sin posibilidad de interceptación
- Irreversible: lo escrito en un bloque no puede borrarse (salvo tras un ataque del 51%)

Características económicas

- Gran volatilidad desincentiva el uso como moneda
- Mucho más uso como activo de inversión
- ¿Gastarías una moneda que se revaloriza un
14.000 %
en 10 años?
- Ojo: muy volátil. También pérdidas del 80% en un año concreto.

Problemas

- Bitcoin es una red lenta y cara: algunas transacciones tardan muchos minutos en confirmarse. Las transacciones tienen costes superiores a las comisiones bancarias o de VISA.
- Transacciones no revocables: una vez firmada, no hay forma de deshacerla. No hay red de seguridad.
- Volatilidad del precio: No tiene nada que lo respalde, y se trata de algo completamente virtual. Fluctuaciones muy grandes
- Consumo eléctrico: el consumo de la red es enorme. Es muy poco eficiente energéticamente.

Minería de bitcoins

Power demand ☐ Annualised consumption

Historical Bitcoin network power demand

Select an area by dragging across the lower chart



19 GW
Consumo
Valle
De
ESPAÑA

<https://ccaf.io/cbnsi/cbeci>

Más palabrejas

- Red Lightning: Una red secundaria para realizar múltiples transacciones y anotar sólo el balance final.
- Fork: cuando no hay consenso frente a un cambio, se bifurca el blockchain (Bitcoin vs Bitcoin Cash)
- Cold wallet: cartera que no tiene sus claves guardadas en un ordenador on-line (papel)
- Litecoin, Ethereum, Dogecoin... y 300 más
- NFT
- Smart Contracts

Exchanges

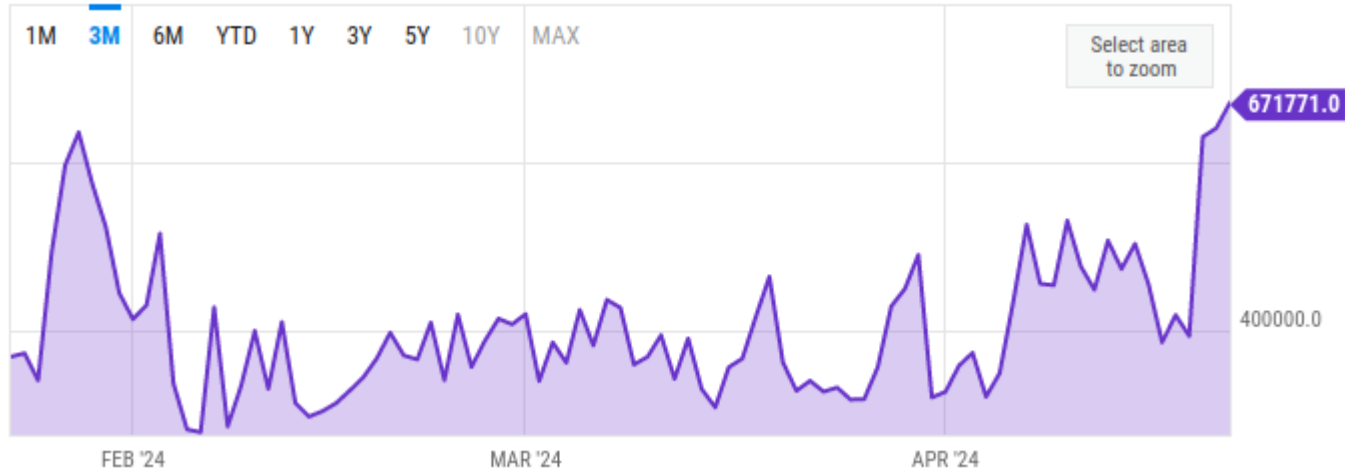
- Empresas de compra/venta de monedas, funcionan como la bolsa: depósito de moneda virtual o fiat, compras y vendas.
- Hasta hace poco: sin regulación/supervisión
- Fraudes / malas gestiones:
 - MTGOX (2014, 480 M\$, 850.000 BTC): OJO: movimiento 2022
 - FTX (2022, pérdidas valoradas en 8.000 M\$)
- Exchanges regulados (Kraken, Blockchain, Crypto.com, etc).

Bitcoin físico

- Hasta 2013, un usuario con alias “Casascius” hizo unas monedas físicas que llevaban dentro las claves de una cartera.
- Dejó de venderlas cuando el gobierno USA le informó de las obligaciones legales...
- Llegó a hacer una moneda de 500 BTC (10.000 USD al cambio)

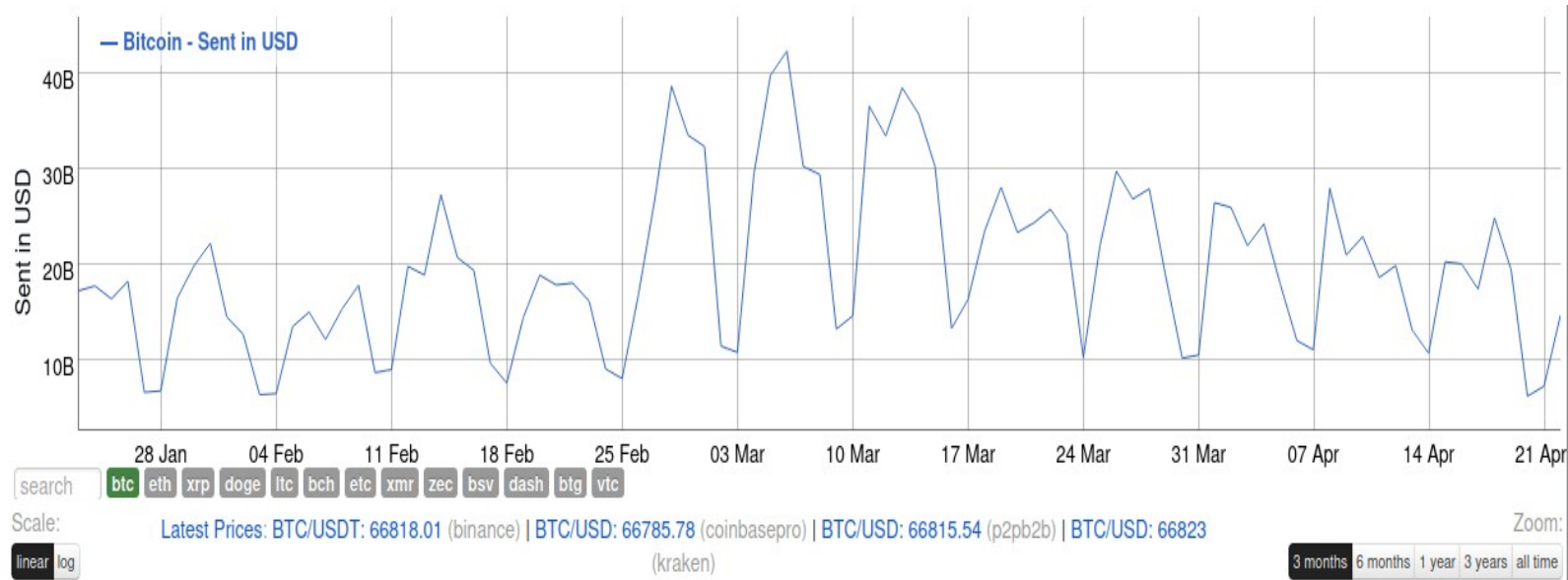


Algunos números



Entre 300.000 y 900.000
transacciones diarias

Algunos números



Entre 6.000 y 40.000 millones de USD diarios
Ojo a patrón lunes-viernes
Máximo: 14/9/2021 → 383.329 millones de USD

Algunos números: Exchanges



Capitalización: 1,32 billones USD (trillones USA)
Volumen 23 abril 2024: 25.360 millones USD

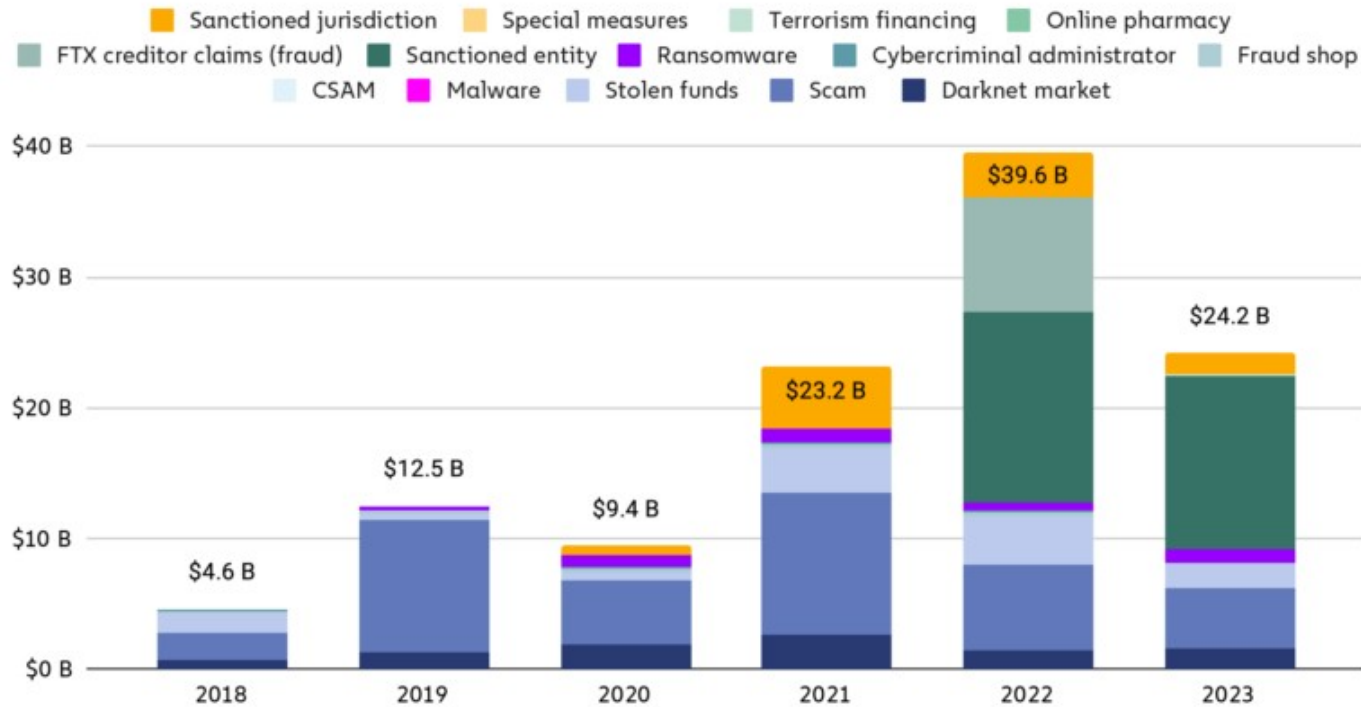
Problemas bitcoin

- Aceptación legal: adopción progresiva. SEC acaba de aceptar ETFs en bitcoins. India, EEUU, Canadá, Suiza, Japón...
- Usos ilícitos: el anonimato llama a los usos ilícitos. Principal moneda para pago de extorsiones.



Problemas criptomonedas

Total cryptocurrency value received by illicit addresses, 2018 - 2023



© Chainalysis

Ataques

- 51%: si una entidad controla el 51% del hashrate, puede generar su propio consenso.
- Doble gasto: mandar bitcoins a pagar y a la vez a la cartera.
- Minado avaricioso: Extender la cadena sin publicarla, para ser el único que pueda minar y/o doble gasto
- Ataques a nodos: manipulación de la hora y de conexiones al resto de la red
- Ataques al id de transacción (ya mitigados / solucionados)

Ataque 51%



Demo time



Anonimato y transparencia

- Sólo se publican direcciones de carteras, nunca datos personales
- Las direcciones de carteras pueden cambiar en cada transacción (una misma cartera puede genera múltiples direcciones distintas)
- Todos los nodos de la red reciben información de las transacciones, verifican y transmiten. Los “mineros” las añaden al bloque (ver <https://mempool.space>).

Anonimato y transparencia

- Para poder identificar a una persona detrás de una transacción hace falta:
 - Tener monitorizados los nodos de la red a los que se conecta y revisar las direcciones que usa
 - Cazarlo en el momento de hacer el paso a moneda fiat y que el exchange comparta información
 - Pillarlo publicando una dirección de bitcoin relacionada

10.000 bitcoins de MTGox



Ki Young Ju

@ki_young_ju



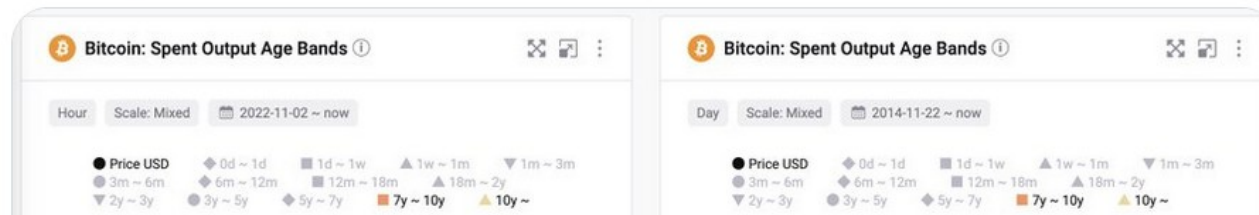
7-year-old 10,000 \$BTC moved today.

No surprise, it's from criminals, like most of the old Bitcoins. It's the BTC-e exchange wallet related to the 2014 Mt. Gox hack.

They sent 65 BTC to @hitbtc a few hours ago, so it's not a gov auction or something.

cryptoquant.com/asset/btc/char...

Traducir post



Anonimato y transparencia

- Agrupamiento de direcciones: intentar asociar distintas direcciones a una misma cartera, y ver dónde se usan todas ellas
- Análisis de transacciones relacionadas: Intentar descubrir patrones de transacciones (por ejemplo, siempre que $A \rightarrow B$, $C \rightarrow D$)
-

Futuro del bitcoin y otros cryptos



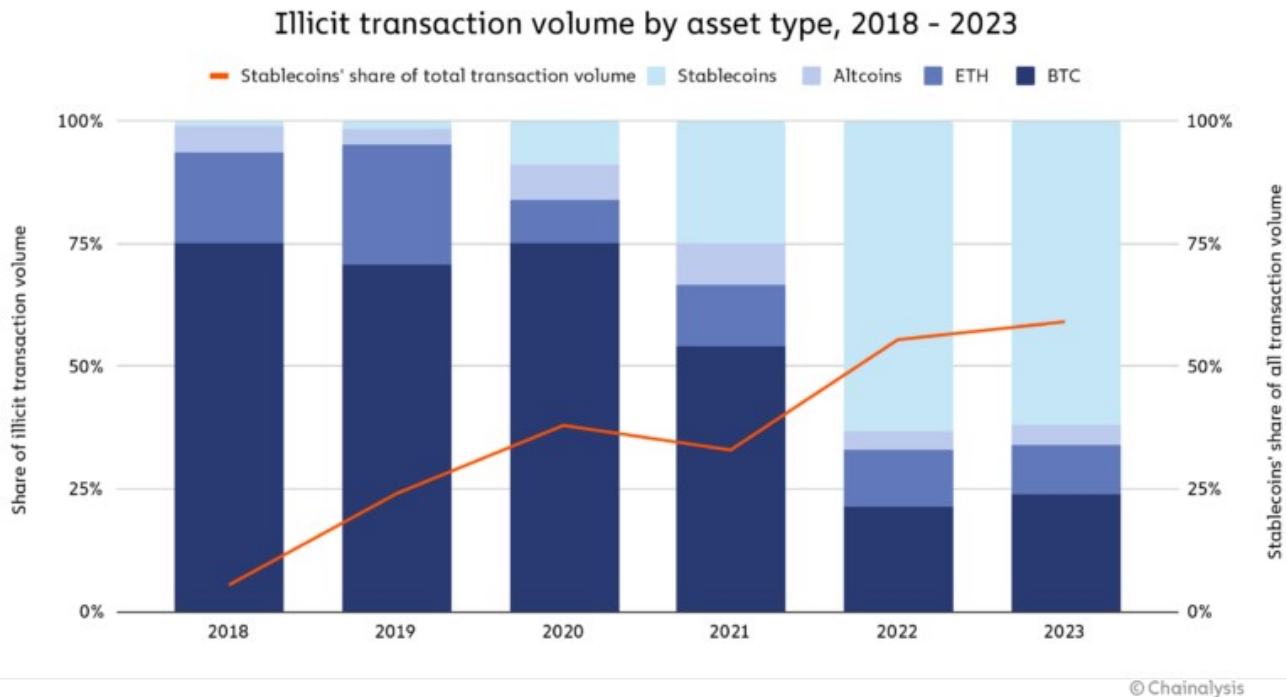
Futuro del bitcoin y otros cryptos

- Adopción cada vez mayor: regulación y negocios
- Distintos cryptos para distintas funcionalidades:
 - Ventas al por menor más rápidas y con menos comisiones
 - NFTs y Smart Contracts
 - Mercados específicos
- Bitcoin sigue siendo el rey
- Inestabilidad de monedas fiat
- Problema principal bitcoin: consumo energético

Futuro del bitcoin

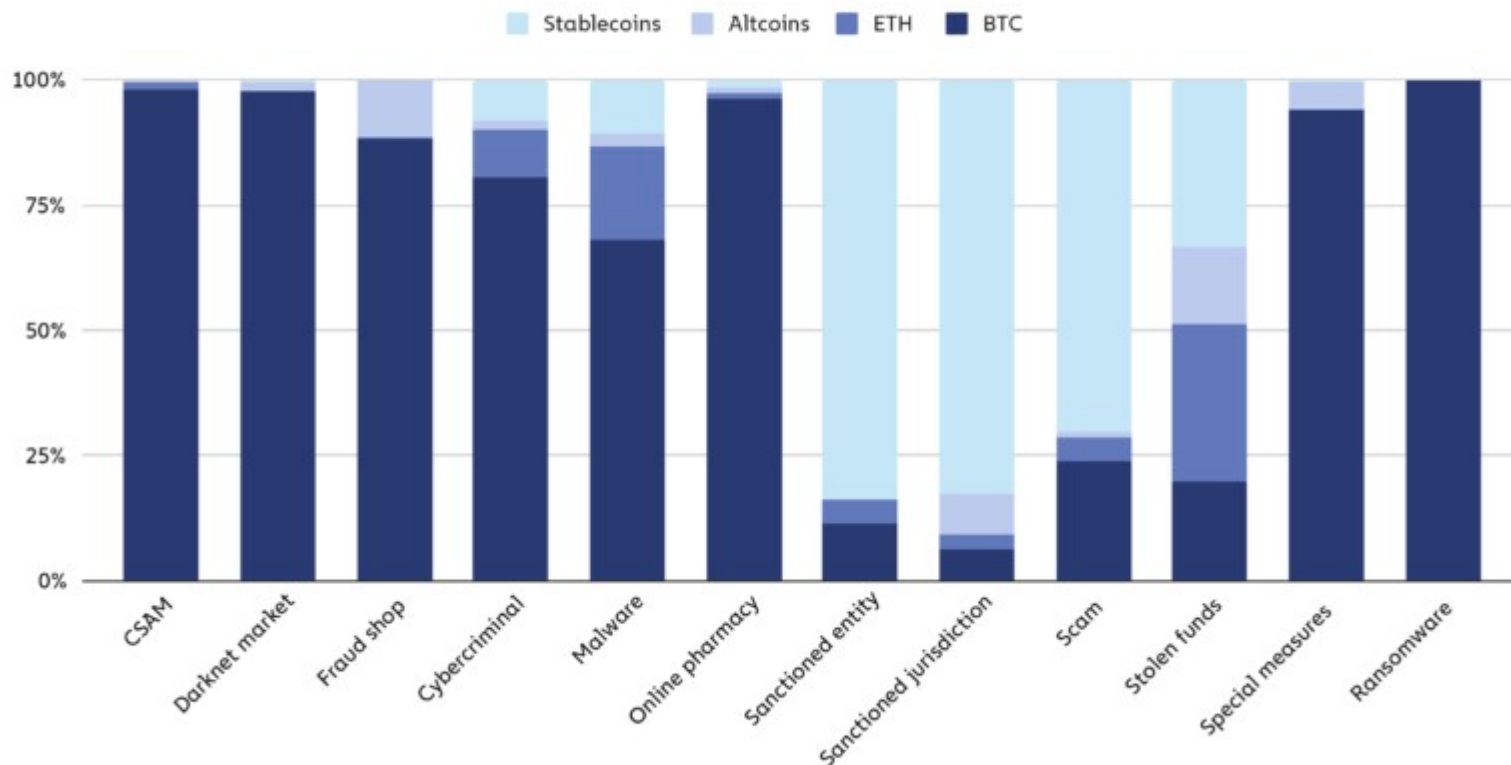
- Poco probable que se use como medio de pago B2C
 - Lento y caro
 - Soluciones más cómodas y seguras
- Va ganando terreno como activo y medio de pago pseudoanónimo
- Muy volátil a corto plazo. Incierto a largo plazo
- Aunque sigue siendo usado en transacciones ilícitas, van cambiando a *stablecoins* (63% en 2023)

Futuro del bitcoin y otros cryptos



Futuro del bitcoin y otros cryptos

Illicit transaction volume by crime category and asset type, 2023



© Chainalysis

Herramientas de análisis

- Gratuitas:
 - <https://www.blockchain.com/explorer>
 - <https://www.bitlisten.com/>
 - <https://blockchair.com>
 - <https://mempool.space>
 - <https://www.bitcoinwhoswho.com>
 - <https://platform.arkhamintelligence.com>
- <https://www.chainalysis.com>
- <https://www.elliptic.co/>
- <https://www.trmlabs.com/>
- <https://crystalintelligence.com/>
- <https://www.anchain.ai/>



64661.94 USD / BTC
Coinbase

BitListen

[Hide Interface]

Realtime Bitcoin transaction visualizer. (Formerly 'Listen To Bitcoin').
Most donations get highlighted: [listendqWJ1mKvrdRUQZDL2F3tVDDyKdj](#)
By Maximilian Laumeister • [Contact](#) • [Source Code](#)





Ejemplo

- Buscamos por cantidad en <https://blockchair.com/bitcoin/outputs>
- Obtenemos el id de transacción
<https://blockchair.com/bitcoin/transaction/b57719827bbe062bf0aede0ef8701986600be5c7bd655b94d9b5b31f546ad0ef>
- Vemos la dirección de origen:
1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g
- Buscamos en varias páginas esta dirección (incluso google)
- <https://www.bitcoinwhoswho.com/address/1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g>
- <https://cryptscam.com/es/detail/1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g>
- <https://platform.arkhamintelligence.com/explorer/address/1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g>



Ejemplo

**Post**
John Connor
@JohnCon54897907

this address has stolen several million bitcoin of which I am a victim! Is there any way of going back to the wrongdoers?
1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g :
1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g QR code Total Received:
7378454.72332449 Total Sent: 7376632.79799721

3:52 p. m. · 28 mar. 2019

 2    



Responder

**John Connor** @JohnCon54897907 · 28 mar. 2019
Final Balance: 1821.92532728 Total transactions: 131587 : site:bitref.com/1Kr6QSydW9bFQG...

**Bitcoin Who's Who** @BitcoinWhosWho · 2 abr. 2019
That's @bitfinex bitcoinwhoswho.com/address/1Kr6QS...



Ejemplo

- Buscamos por cantidad en <https://blockchair.com/bitcoin/outputs>
- Obtenemos el id de transacción
<https://blockchair.com/bitcoin/transaction/b57719827bbe062bf0aede0ef8701986600be5c7bd655b94d9b5b31f546ad0ef>
- Vemos la dirección de origen:
1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g
- Buscamos en varias páginas esta dirección (incluso google)
- <https://www.bitcoinwhoswho.com/address/1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g>
- <https://cryptscam.com/es/detail/1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g>
- <https://platform.arkhamintelligence.com/explorer/address/1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g>

Muchas gracias
ediaz@ultreia.es



Dirección
Para
donaciones

bc1q6fhtu2ejgjjqzh9t5m20edxtn541pqr1mmt52