
Criptomonedas: terminología, mitos y verdades

Neko Workspace - Emilio Almansi - Abril 2019

Terminología

Terminología

Criptomoneda

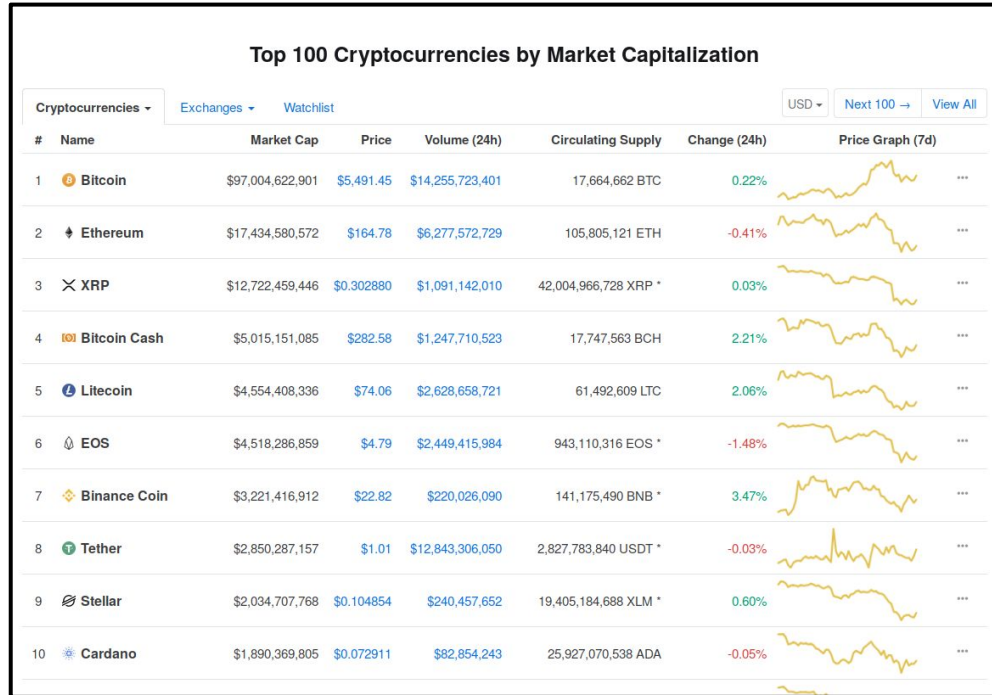


Fig 1. Criptomonedas

Terminología

Criptomonedas, Bitcoin

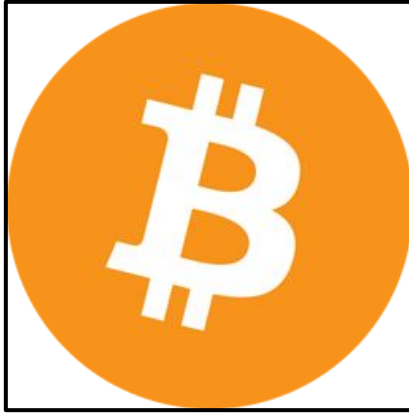


Fig 2. Bitcoin

Terminología

Criptomoneda, Bitcoin, Altcoin

2		Ethereum	ETH
3		Bitcoin Cash	BCH
4		Litecoin	LTC

Fig 3. Altcoins

Terminología

Criptomonedas, Bitcoin, Altcoin, Transacción, Blockchain

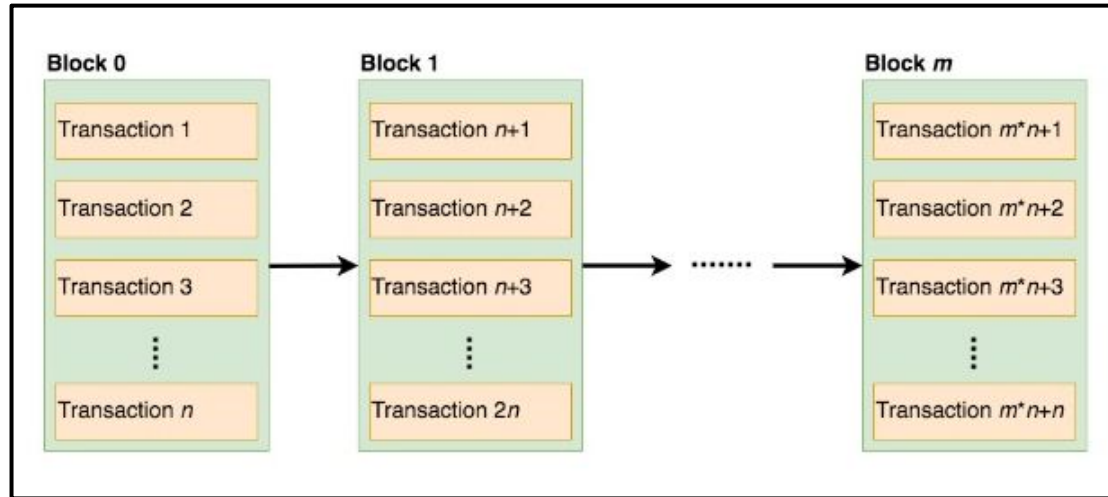


Fig 4. Blockchain

Terminología

Criptomonedas, Bitcoin, Altcoin, Transacción, Blockchain,
Whitepaper, Decentralización, Algoritmo de consenso

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

Fig 5. Whitepaper

Terminología

Criptomonedas, Bitcoin, Altcoin, Transacción, Blockchain, Whitepaper, Decentralización, Algoritmo de consenso

Nodo, Minero



Fig 6. Minería

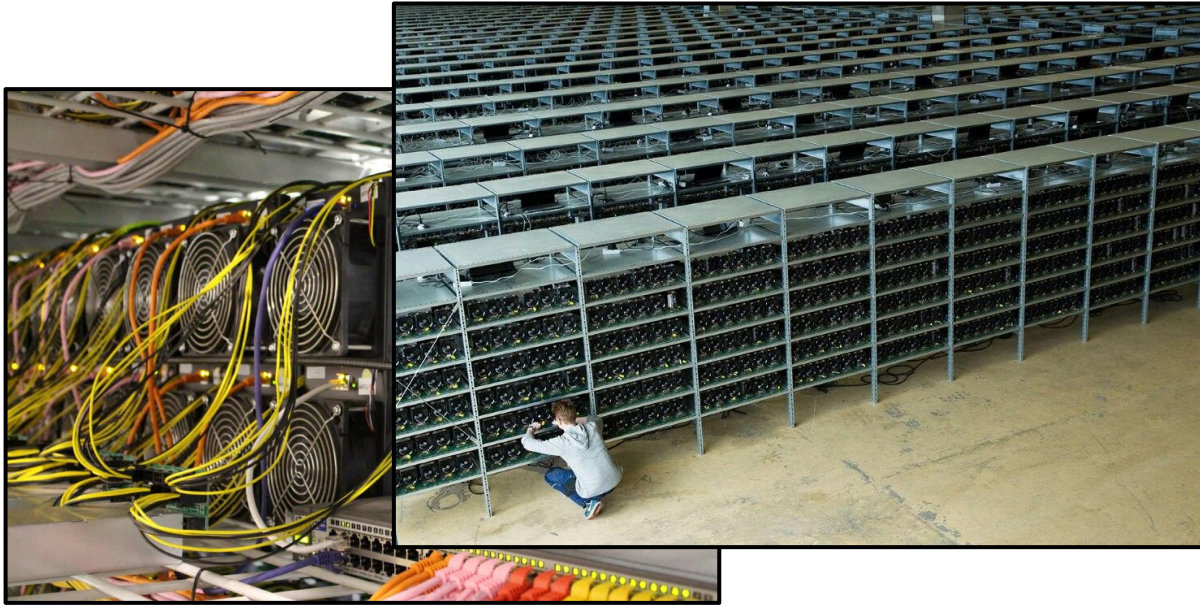


Fig 6. Minería



Fig 6. Minería

Terminología

Criptomonedas, Bitcoin, Altcoin, Transacción, Blockchain,
Whitepaper, Decentralización, Algoritmo de consenso

Nodo, Minero, Explorador

BlockExplorer

NewsBitcoin cashConference ScheduleBlocksStatus

Buy Bitcoin with CCI

Search for block, transaction or address

Conn 60 - Height 491224

Scan

USD

Latest Blocks


Height	Age	Transactions	Mined by	Size
491224	11 minutes ago	2259		972566
491223	11 minutes ago	1952		983737
491222	21 minutes ago	2554		963398
491221	25 minutes ago	2274		887501
491220	34 minutes ago	1630		984002

See all blocks


Latest Transactions

Hash	Value Out
e18383134e81094f26ae21b87d2f17b35d5a141245...	5402.35 USD
fce307758dee5887f67dedc7233d887594ae4aa0d8c...	1087.42 USD
7d5e1547ac85593618b53f85ab75888495f74102286...	3.55 USD
6773f9ef51a17c5b136a17df2cf99ae531450bc65329...	951.85 USD
96bf88a5923c36f76cc85ae98be9801e4ca82212c457...	29.67 USD
c6bb4f78f56d1611e6078ca3d07986d8e3bf67a6271...	1184.3 USD
c47723038a02ae147d5bac7f8cc34036d155623120...	3402.06 USD


News



The anatomy of a poorly executed ICO scam: Langpie



London to host the ICO conference – ICO Event London 2017



BLOCKBALI – BBS Blackarrow's Blockchain Conference in Bali, Indonesia on 27th October 2017

About Block Explorer

Bitcoin Block Explorer is an open source web tool that allows you to view information about blocks, addresses, and transactions on the Bitcoin blockchain. The source code is on GitHub.

What is bitcoin?

Public Bitcoin API: Machine readable stats & blockchain info can be accessed directly through the REST and Websockets APIs.

Fig 7. Explorador

18

Terminología

Criptomonedas, Bitcoin, Altcoin, Transacción, Blockchain,
Whitepaper, Decentralización, Algoritmo de consenso

Nodo, Minero, Explorador, Exchange, Broker

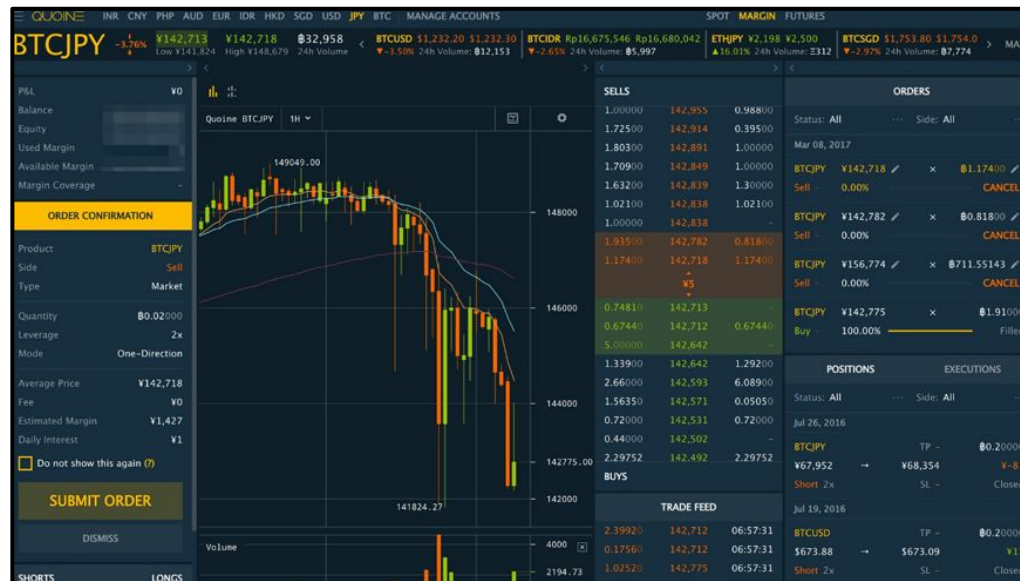


Fig 8. Exchange

Terminología

Criptomonedas, Bitcoin, Altcoin, Transacción, Blockchain, Whitepaper, Decentralización, Algoritmo de consenso

Nodo, Minero, Explorador, Exchange, Broker

Wallet, Dirección o address

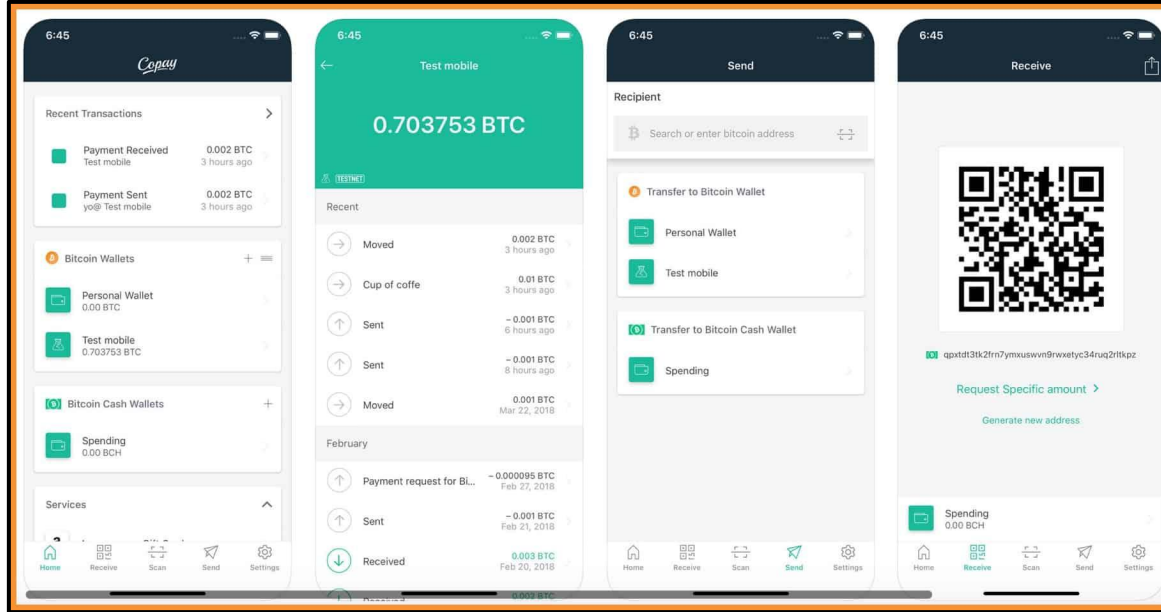


Fig 9. Wallet

Terminología

Criptomonedas, Bitcoin, Altcoin, Transacción, Blockchain, Whitepaper, Decentralización, Algoritmo de consenso

Nodo, Minero, Explorador, Exchange, Broker

Wallet, Dirección o address, Claves públicas/privadas, Seed

"Deterministic wallet" is a neat and secure way to generate a public/private keypair out of a human readable seed. Luckily Bitcoin is based on Elliptic curve cryptography which means seeds can be both short and secure.

Seed (12 words x 11 bits = 132 bits of entropy)

constant forest adore false green weave stop guy fur freeze giggle clock

5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nEB3kEsreAnchuDf

Private key

1BgGZ9tcN4rm9KBzDn7KprQz87SZ26SAMI

Public key

Fig 10. Claves, seed

Terminología

Criptomonedas, Bitcoin, Altcoin, Transacción, Blockchain, Whitepaper, Decentralización, Algoritmo de consenso

Nodo, Minero, Explorador, Exchange, Broker

Wallet, Dirección o address, Claves públicas/privadas, Seed

Paper wallets, Hardware wallets



Fig 11. Paper/hardware wallets



Fig 11. Paper/hardware wallets

Cómo funciona?

Un **usuario** puede crear una **wallet** en cualquier dispositivo, y utilizarla para **enviar y recibir** criptomonedas. Crear una wallet y recibir dinero es gratuito. Para enviar dinero es necesario conocer una **dirección** de la wallet destino, y pagar un **fee** destinado a la **verificación** de la transacción.

Cómo funciona?

Un **usuario** puede crear una **wallet** en cualquier dispositivo, y utilizarla para **enviar y recibir** criptomonedas. Crear una wallet y recibir dinero es gratuito. Para enviar dinero es necesario conocer una **dirección** de la wallet destino, y pagar un **fee** destinado a la **verificación** de la transacción.

Las criptomonedas se pueden obtener mediante la **minería**, a cambio de **bienes y servicios**, o se pueden comprar en un **exchange** o a un particular.

Cómo funciona?

Los **mineros** generan **bloques**, que contienen las **transacciones** de los usuarios. A cambio, reciben una **recompensa** compuesta por los fees más una recompensa base por el bloque.

Cómo funciona?

Los **mineros** generan **bloques**, que contienen las **transacciones** de los usuarios. A cambio, reciben una **recompensa** compuesta por los fees más una recompensa base por el bloque.

Los **nodos** de la red reciben los bloques nuevos y los **transmiten** a los demás nodos. Entre ellos, se ponen de acuerdo sobre cuáles bloques son **válidos** mediante un **algoritmo de consenso**.

Cómo funciona?

La minería es el único mecanismo para **emitir** nuevas criptomonedas. La cantidad de monedas que se emiten por cada bloque generado está determinada por el **protocolo**.

Cómo funciona?

La minería es el único mecanismo para **emitir** nuevas criptomonedas. La cantidad de monedas que se emiten por cada bloque generado está determinada por el **protocolo**.

En Bitcoin, cada cuatro años se reduce la cantidad de monedas que se crean por bloque (**halving**). El último bitcoin se va a emitir cerca del **año 2140**, completando un total de **21.000.000**.

Cómo funciona?

La red es completamente **pública** y abierta a la participación de cualquier persona con acceso a internet. Técnicamente, cualquiera puede modificar la blockchain creando nuevos bloques y emitiendo nuevas monedas.

Cómo funciona?

La red es completamente **pública** y abierta a la participación de cualquier persona con acceso a internet. Técnicamente, cualquiera puede modificar la blockchain creando nuevos bloques y emitiendo nuevas monedas.

Para prevenir abuso, la generación de bloques requiere consumir energía (**Proof-of-Work**). El sistema se auto-regula de manera tal que los bloques se generen, en promedio, cada **10 minutos**.

Cómo funciona?

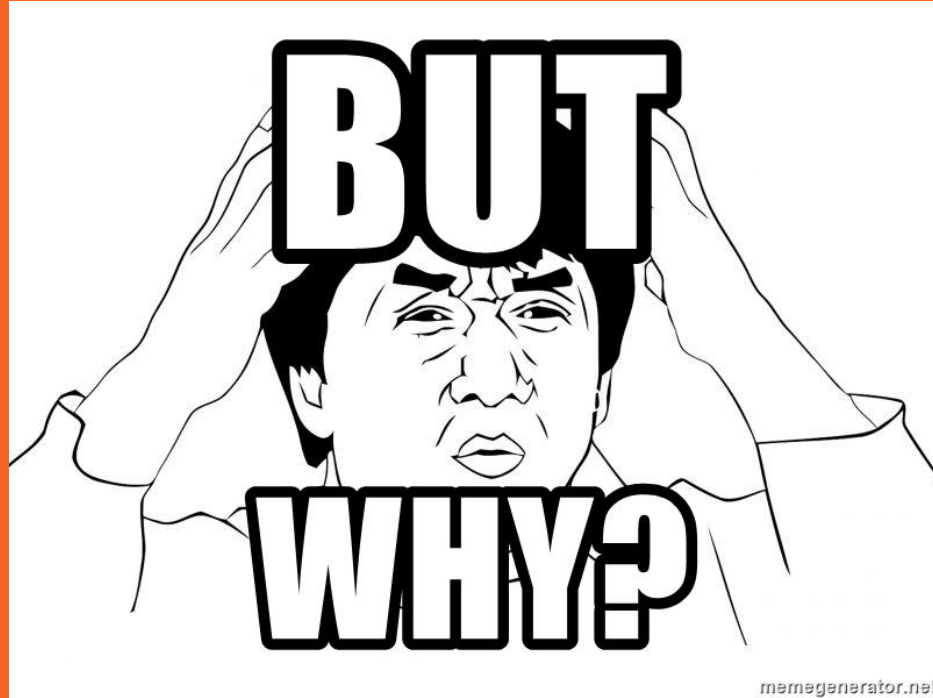
A mayor cantidad de energía invertida en la red mediante minería (**hashrate**), mayor la injerencia sobre la red y mayor la recompensa.

Cómo funciona?

A mayor cantidad de energía invertida en la red mediante minería (**hashrate**), mayor la injerencia sobre la red y mayor la recompensa.

Hoy en día, la red de Bitcoin tiene 100.000 veces más poder de cómputo que las 500 supercomputadoras más importantes del mundo combinadas.

Demo



Para qué todo esto?

Orígenes.

Cypherpunks, criptografía, privacidad.

Libertad económica.

Descentralización.

Seguridad. Inmutabilidad.

Utilidad.

Para qué sirve?

Remesas, transferencias internacionales. Son bienes que se puede comprar y vender por todo el mundo.

Para qué sirve?

Remesas, transferencias internacionales. Son bienes que se puede comprar y vender por todo el mundo.

Resguardo de valor. Medio de intercambio.

Para qué sirve?

Remesas, transferencias internacionales. Son bienes que se puede comprar y vender por todo el mundo.

Resguardo de valor. Medio de intercambio.

Inversión especulativa. Medio de financiamiento para empresas (ICOs).

Para qué sirve?

Remesas, transferencias internacionales. Son bienes que se puede comprar y vender por todo el mundo.

Resguardo de valor. Medio de intercambio.

Inversión especulativa. Medio de financiamiento para empresas (ICOs).

Aplicaciones no monetarias, registros de propiedad, tokenización de bienes, organizaciones descentralizadas.

Mitos y verdades

Mitos y verdades

Bitcoin sirve para facilitar actividades ilegales.

Bitcoin **solo** sirve para facilitar actividades ilegales.

Bitcoin es anónimo.

Bitcoin es auditable y trazable.

La verdadera innovación tecnológica es la blockchain, no Bitcoin.

Mitos y verdades

Bitcoin sirve para facilitar actividades ilegales. (cierto)

Bitcoin **solo** sirve para facilitar actividades ilegales.

Bitcoin es anónimo.

Bitcoin es auditable y trazable.

La verdadera innovación tecnológica es la blockchain, no Bitcoin.

Mitos y verdades

Bitcoin sirve para facilitar actividades ilegales. (cierto)

Bitcoin **solo** sirve para facilitar actividades ilegales. (falso)

Bitcoin es anónimo.

Bitcoin es auditable y trazable.

La verdadera innovación tecnológica es la blockchain, no Bitcoin.

Mitos y verdades

Bitcoin sirve para facilitar actividades ilegales. (cierto)

Bitcoin **solo** sirve para facilitar actividades ilegales. (falso)

Bitcoin es anónimo. (falso)

Bitcoin es auditable y trazable.

La verdadera innovación tecnológica es la blockchain, no Bitcoin.

Mitos y verdades

Bitcoin sirve para facilitar actividades ilegales. (cierto)

Bitcoin **solo** sirve para facilitar actividades ilegales. (falso)

Bitcoin es anónimo. (falso)

Bitcoin es auditable y trazable. (cierto)

La verdadera innovación tecnológica es la blockchain, no Bitcoin.

Mitos y verdades

Bitcoin sirve para facilitar actividades ilegales. (cierto)

Bitcoin **solo** sirve para facilitar actividades ilegales. (falso)

Bitcoin es anónimo. (falso)

Bitcoin es auditable y trazable. (cierto)

La verdadera innovación tecnológica es la blockchain, no Bitcoin. (falso)

Mitos y verdades

Bitcoin es malo para el medio ambiente.

Bitcoin no tiene ningún respaldo.

Las criptomonedas son una inversión muy riesgosa.

Bitcoin solo se puede comprar o tener en unidades enteras.

Bitcoin es lento y caro.

Mitos y verdades

Bitcoin es malo para el medio ambiente. (discutible)

Bitcoin no tiene ningún respaldo.

Las criptomonedas son una inversión muy riesgosa.

Bitcoin solo se puede comprar o tener en unidades enteras.

Bitcoin es lento y caro.

Mitos y verdades

Bitcoin es malo para el medio ambiente. (discutible)

Bitcoin no tiene ningún respaldo. (falso)

Las criptomonedas son una inversión muy riesgosa.

Bitcoin solo se puede comprar o tener en unidades enteras.

Bitcoin es lento y caro.

Mitos y verdades

Bitcoin es malo para el medio ambiente. (discutible)

Bitcoin no tiene ningún respaldo. (falso)

Las criptomonedas son una inversión muy riesgosa. (cierto)

Bitcoin solo se puede comprar o tener en unidades enteras.

Bitcoin es lento y caro.

Mitos y verdades

Bitcoin es malo para el medio ambiente. (discutible)

Bitcoin no tiene ningún respaldo. (falso)

Las criptomonedas son una inversión muy riesgosa. (cierto)

Bitcoin solo se puede comprar o tener en unidades enteras.
(falso)

Bitcoin es lento y caro.

Mitos y verdades

Bitcoin es malo para el medio ambiente. (discutible)

Bitcoin no tiene ningún respaldo. (falso)

Las criptomonedas son una inversión muy riesgosa. (cierto)

Bitcoin solo se puede comprar o tener en unidades enteras.
(falso)

Bitcoin es lento y caro. (discutible)

Más info:

<https://emilio.almansi.me/neko-2>

[019](#)