Curso de Bitcoin y Blockchain

Angela Ocando

¿Qué es Bitcoin?

Bitcoin es una innovadora red de pagos de código abierto y una nueva clase de dinero.

Bitcoin.org

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.

Bitcoin es...

- Seguro
- Inmutable
- Trasparente
- Anónimo
- Descentralizado

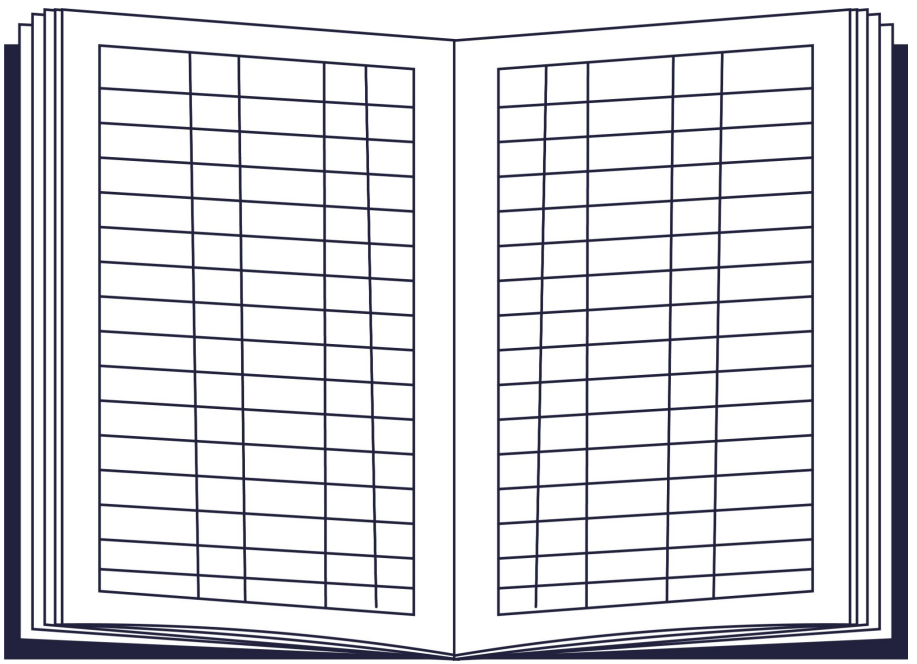
Bitcoin funciona utilizando:

- Blockchain
- Prueba de Trabajo (PoW)
- P2P
- Criptografía

Blockchain

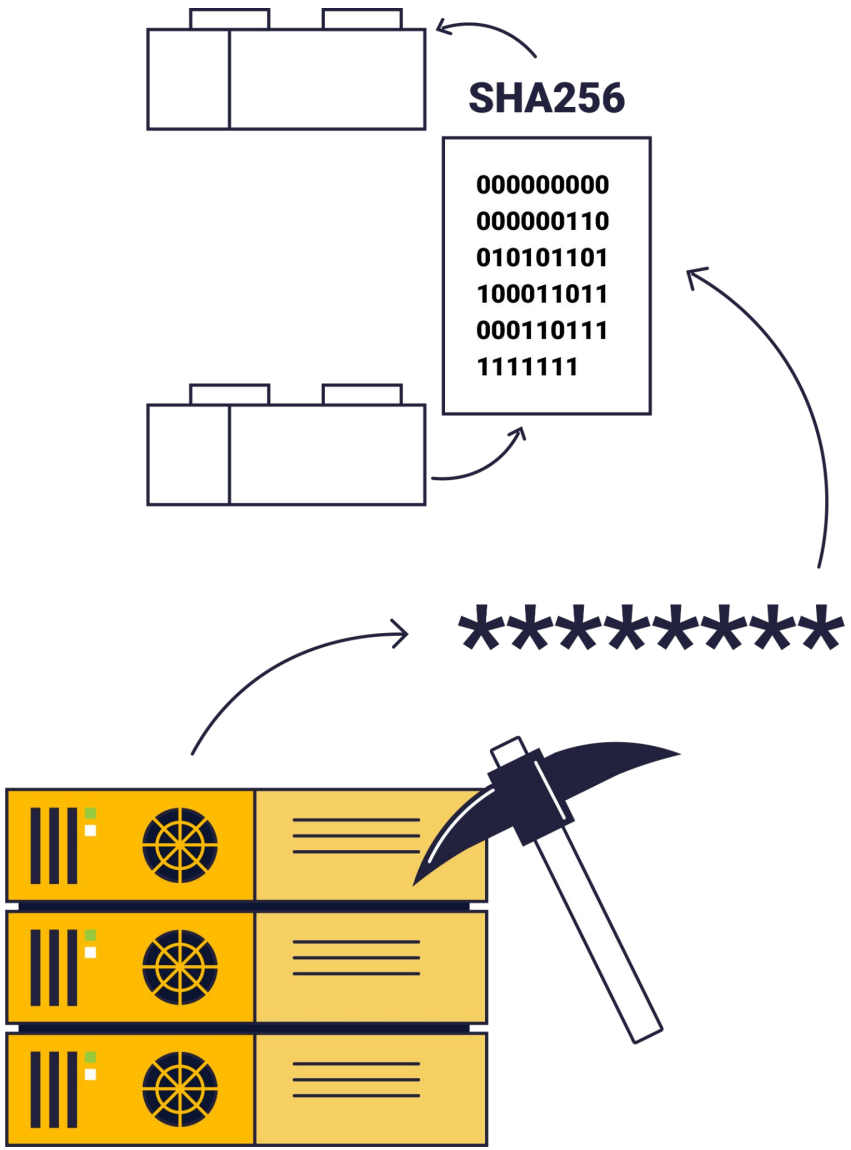
Es una base de datos distribuida en varios nodos de una red.

Cadena de bloques de información.



Prueba de trabajo

Es la búsqueda de un número o variable que permite que se puedan insertar bloques en blockchain y además requieren un nivel de cálculo y cómputo complejo.



Adam Back

Hashcash: el ancestro de PoW

Hashcash - A Denial of Service Counter-Measure

Adam Back
e-mail: adam@cypherspace.org

1st August 2002

Abstract

Hashcash was originally proposed as a mechanism to throttle systematic abuse of un-metered internet resources such as email, and anonymous remailers in May 1997. Five years on, this paper captures in one place the various applications, improvements suggested and related subsequent publications, and describes initial experience from experiments using hashcash.

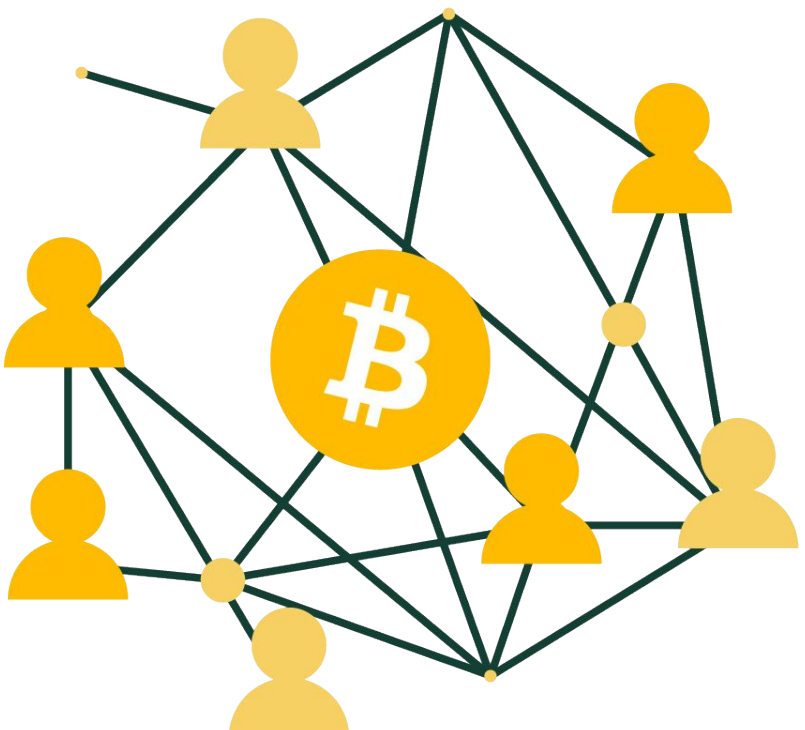
The *hashcash* CPU cost-function computes a token which can be used as a proof-of-work. Interactive and non-interactive variants of cost-functions can be constructed which can be used in situations where the server can issue a challenge (connection oriented interactive protocol), and where it can not (where the communication is store–and–forward, or packet oriented) respectively.

Key Words: hashcash, cost-functions

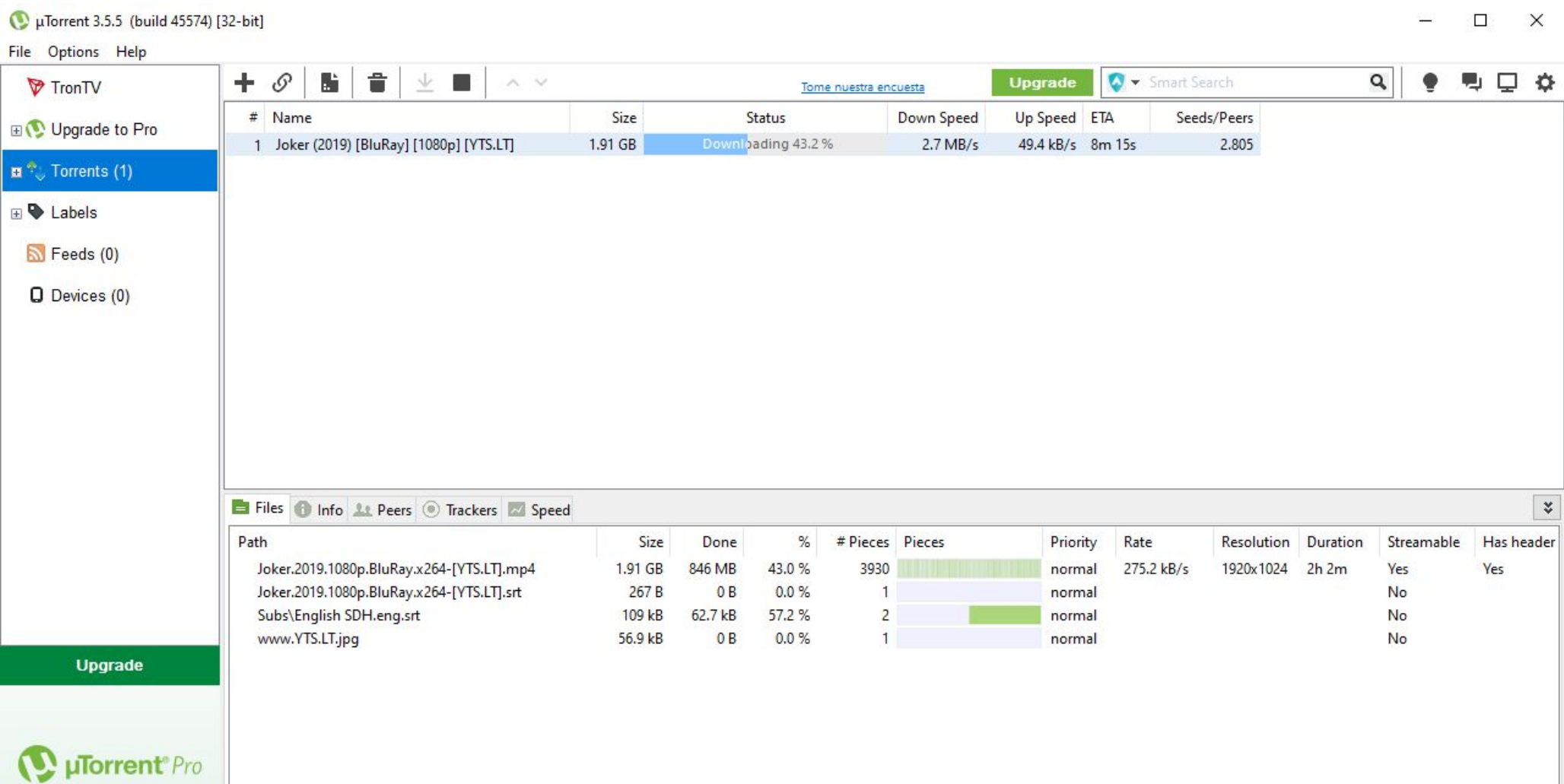
Evitar spam

P2P

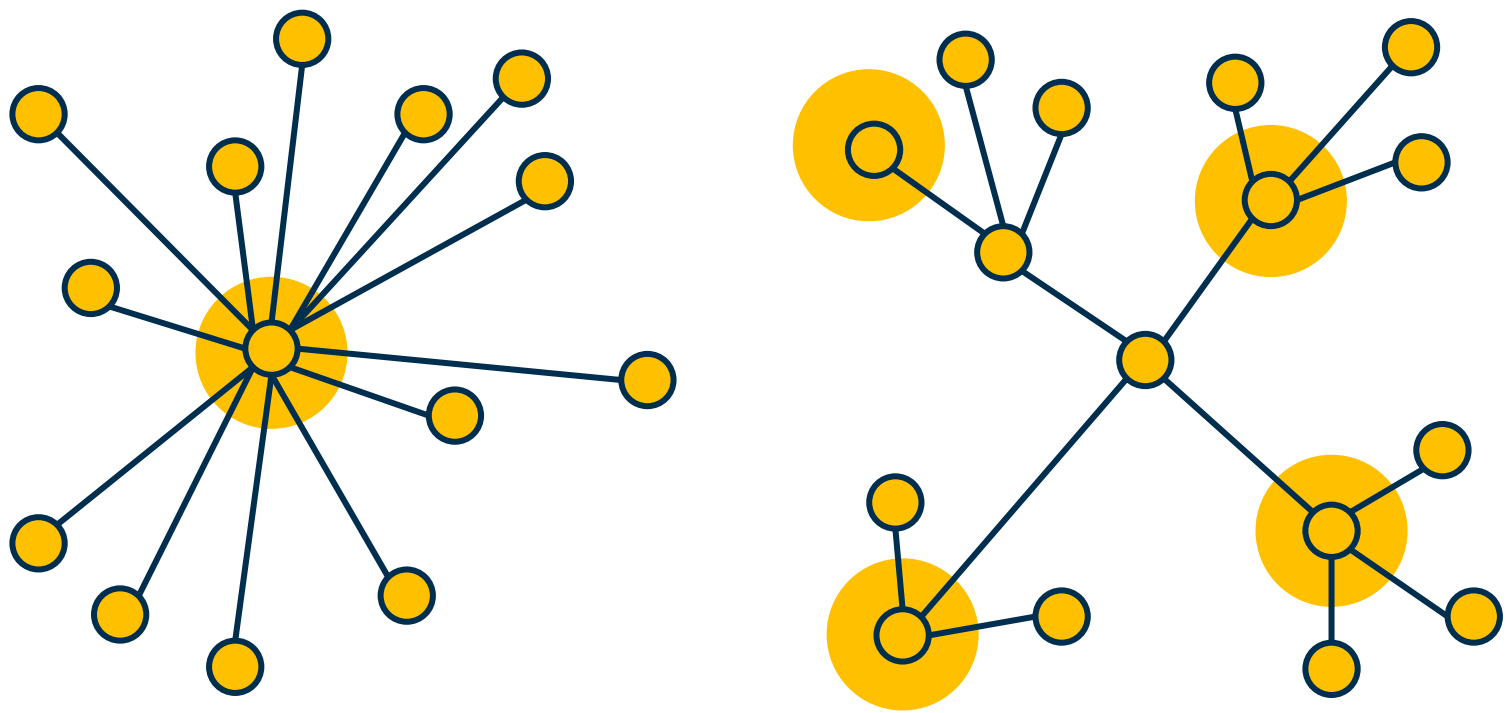
Red de ordenadores o nodos que están conectados entre sí y permiten el intercambio directo de información de igual a igual.



Torrents


µTorrent 3.5.5 (build 45574) [32-bit]
File Options Help
TronTV
Upgrade to Pro
Torrents (1)
Labels
Feeds (0)
Devices (0)
Upgrade
µTorrent Pro
Tome nuestra encuesta
Upgrade
Smart Search
Name Size Status Down Speed Up Speed ETA Seeds/Peers
1 Joker (2019) [BluRay] [1080p] [YTS.LT] 1.91 GB Downloading 43.2 % 2.7 MB/s 49.4 kB/s 8m 15s 2.805
Files Info Peers Trackers Speed
Path Size Done % # Pieces Pieces Priority Rate Resolution Duration Streamable Has header
Joker.2019.1080p.BluRay.x264-[YTS.LT].mp4 1.91 GB 846 MB 43.0 % 3930 normal 275.2 kB/s 1920x1024 2h 2m Yes Yes
Joker.2019.1080p.BluRay.x264-[YTS.LT].srt 267 B 0 B 0.0 % 1 normal No
Subs\English SDH.eng.srt 109 kB 62.7 kB 57.2 % 2 normal No
www.YTS.LT.jpg 56.9 kB 0 B 0.0 % 1 normal No

Servidores descentralizados



Criptografía

Es tecnología utilizada para resguardar la integridad de los datos y así evitar que personas no autorizadas accedan a la información.

Enigma

Las criptomonedas son información que navegan en la web


DECENTRALIZED PEER TO PEER
BITCOIN DIGITAL
METALS
1TROY OZ 999 FINE COPPER MJB MONETARY

Whitepaper

¿Cómo funciona Bitcoin?

Funcionamiento de Blockchain

de bitcoin

Minería

El rol de quienes minan

Minería

Ejecución de PoW.

Resolución de algoritmos complejos para el funcionamiento descentralizado y seguro de Bitcoin a partir de poder de cómputo.

El rol de quienes minan

- Comprueban que las transacciones sean realizadas.
- Certificar que nadie pueda usar dos veces la misma moneda o introducir monedas falsas.
- Crean nuevos bitcoins a partir de la creación de nuevos bloques.
- Reciben una recompensa por el trabajo realizado.

Incentivos

Por su labor, las personas que minan reciben dos tipos de recompensas:

- Al resolver un bloque y emitir nuevos bitcoins.
- Al validar rápidamente transacciones que se incluyen en los bloques.

Resolviendo bloques

- 6.25 BTC (hoy día).
- Comisiones de transacciones.
- Esta recompensa se reduce a la mitad cada vez que se minan 210.000 bloques y se conoce como Halving o aumento de la dificultad de minado.
- Para tener más probabilidades de resolver bloques existen pools de minería.

2024 Tiempo estimado para halving de bloques:

952 días	7 horas	18 minutos	

Fecha estimada: 26 de marzo de 2024

Bloques hasta el halving: 143.843

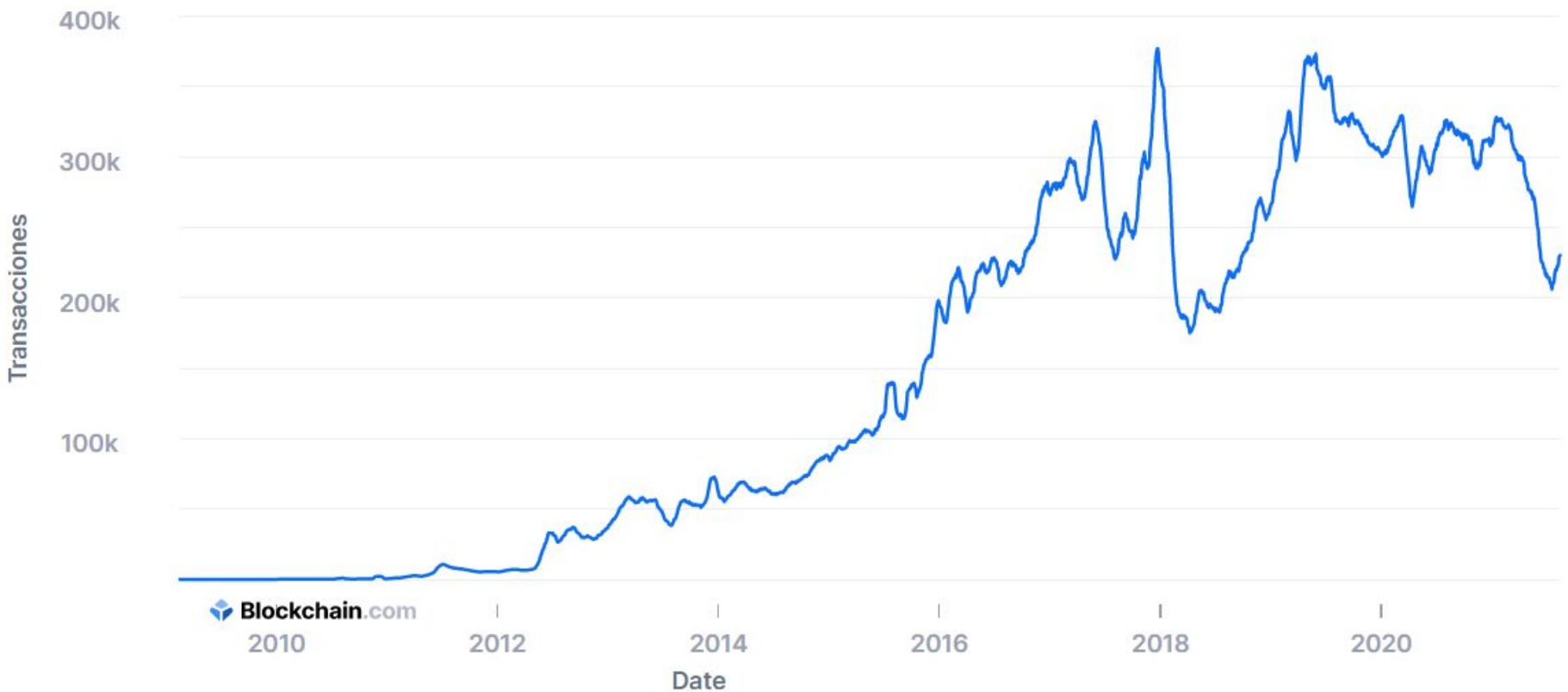
Tomado de: https://www.buybitcoinworldwide.com/es/bitcoin-clock/

Validando transacciones

- Comisiones de transacciones.
- Debido al crecimiento de la red, los mineros priorizan y validan transacciones.
- Evita la posibilidad de ataques a la red.
- En cuanto se minen los 21 millones de bitcoins, será probablemente el proceso que sustente el funcionamiento de la red.

Transacciones confirmadas por día

El número total de transacciones confirmadas por día.



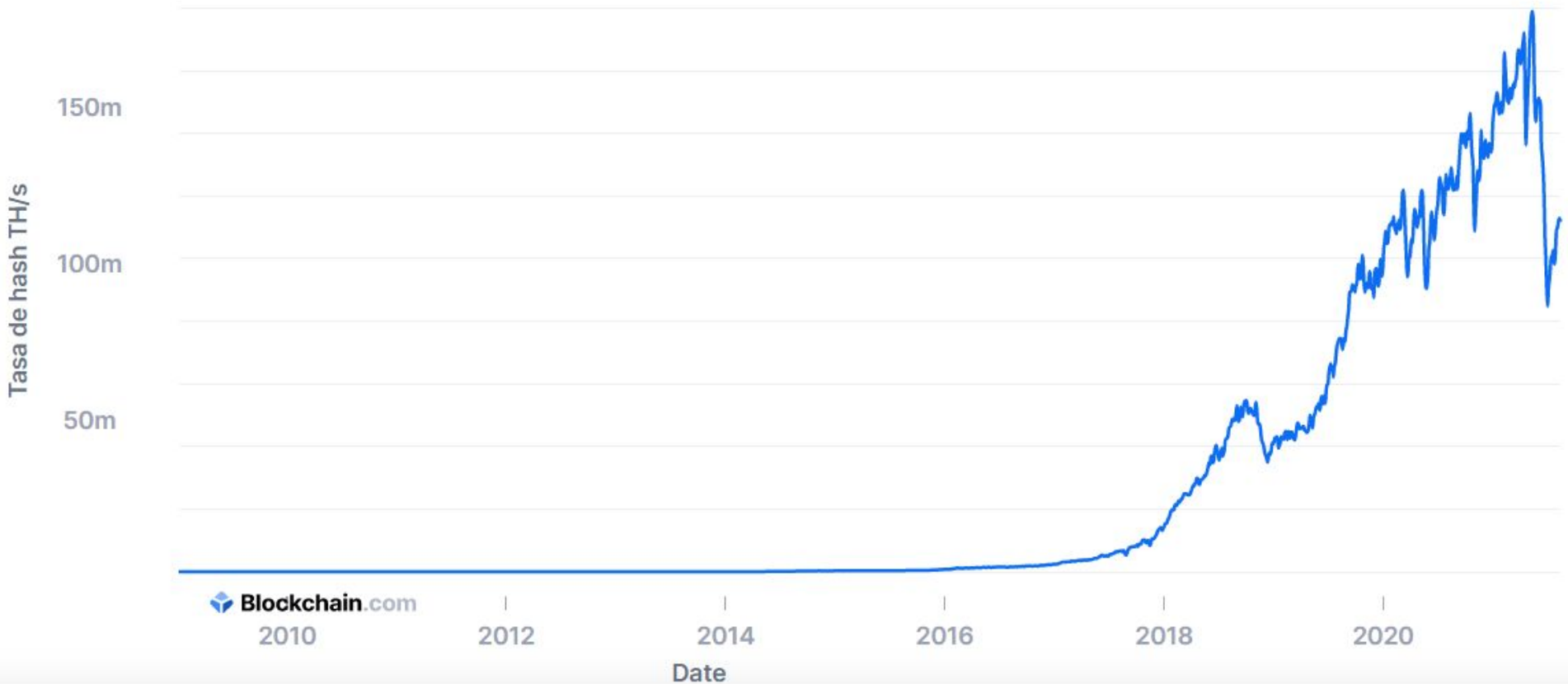
Tasa de Hash

Poder de cómputo total que se utiliza para minar y poder procesar transacciones de Bitcoin (PoW).

Mientras más alto en hashrate mayor la seguridad del ataque y también la complejidad para minar.

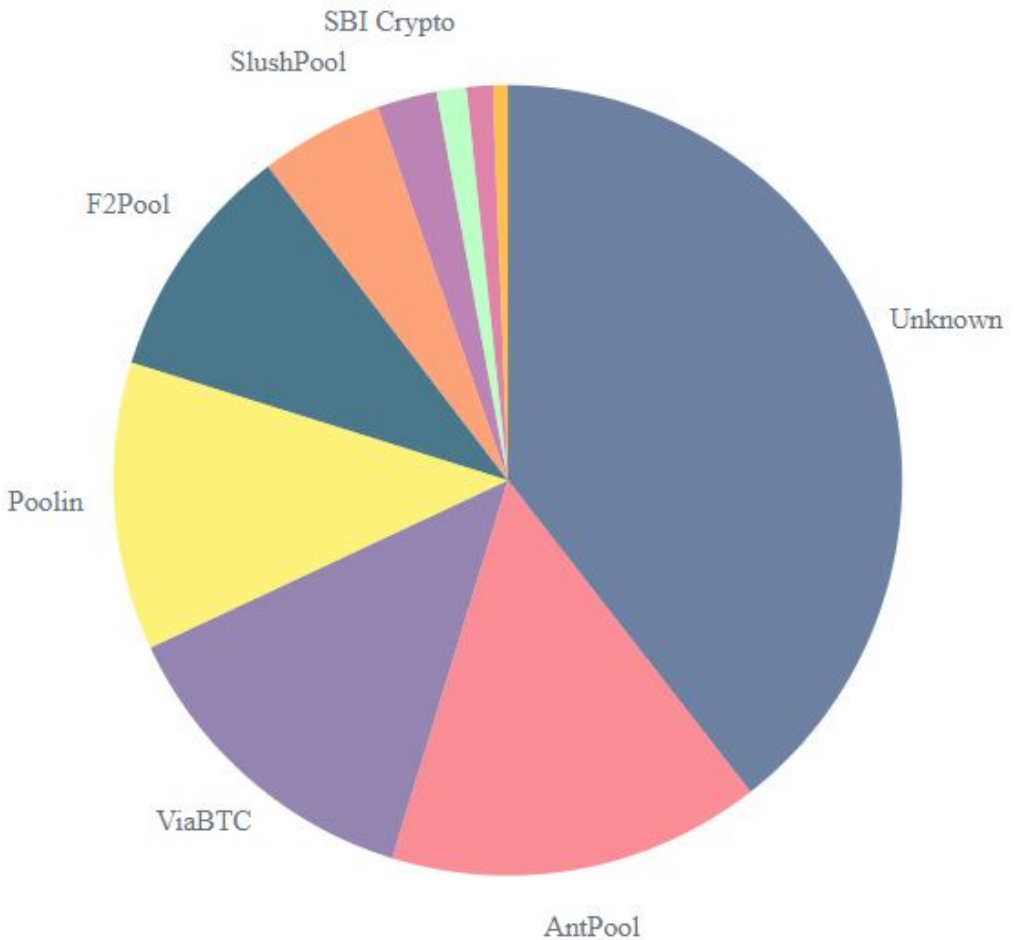
Total tasa de hash TH/s

El número estimado de terahashes por segundo que la red de bitcoin ha realizado en las últimas 24 horas.



Distribución de tasa hash

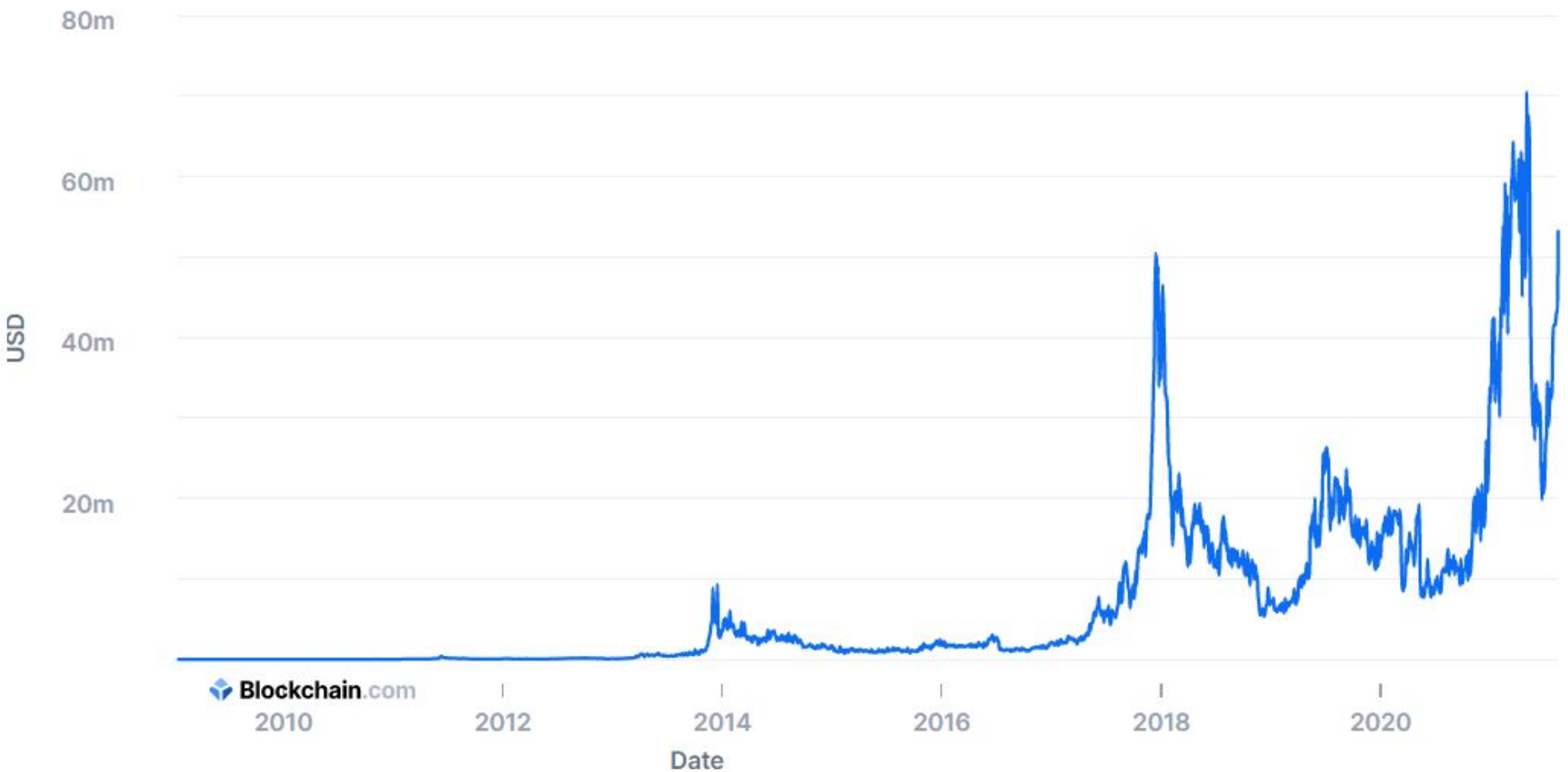
Una estimación de la distribución de la tasa hash entre los pools de minado de mayor tamaño.



24 horas | 48 horas | 4 días

Rendimiento de minador (USD)

Valor total en USD de las recompensas y tasas de transacción de un bloque de Coinbase pagadas a los minadores.



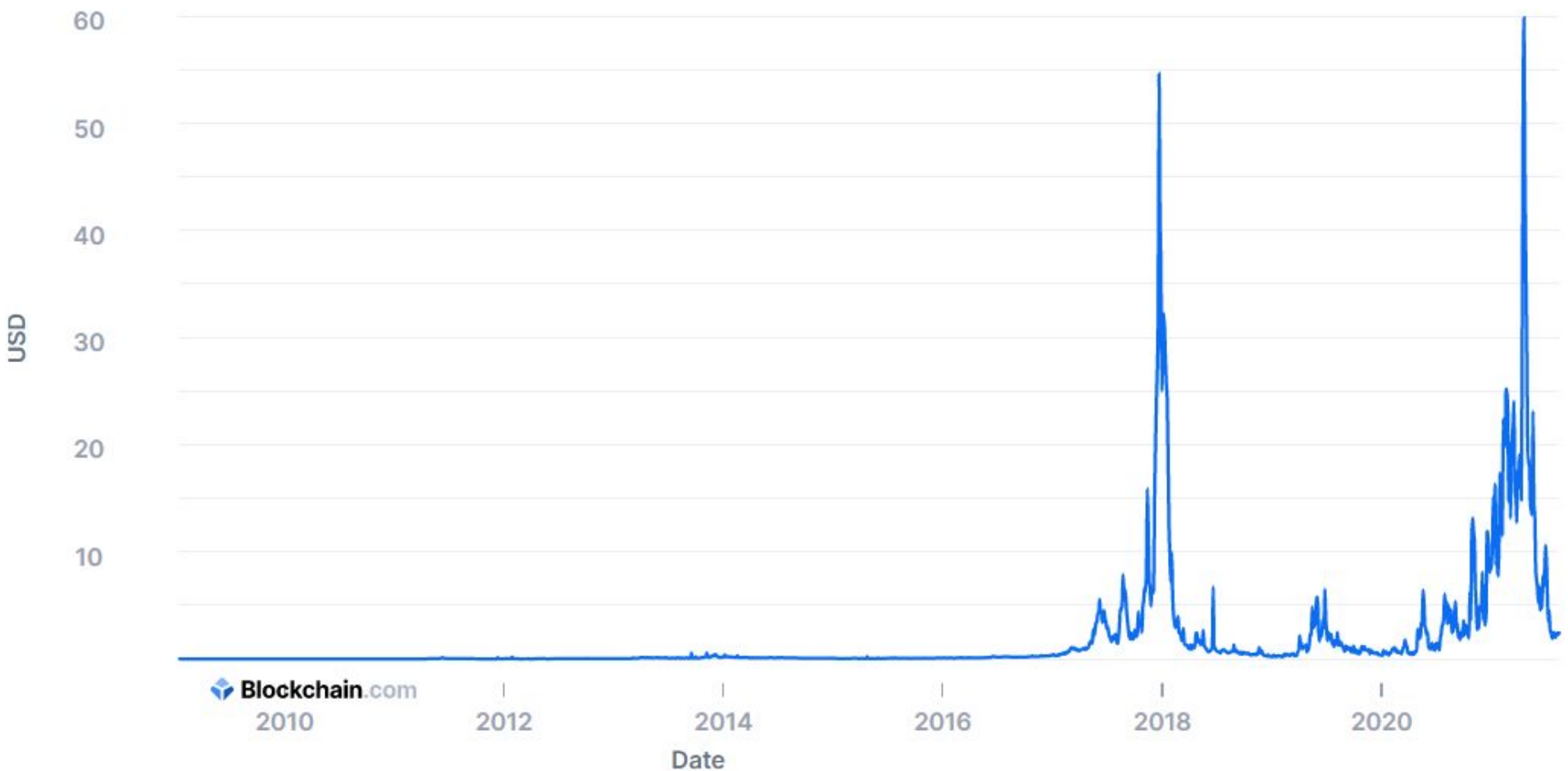
Lightning network

Problemas de escalabilidad

- 7 transacciones por segundo.
- Transacciones lentas.
- Altos costos transaccionales.

Tasas por transacción (USD)

Tasa de transacción media en USD por transacción.



Lightning Network

Scalable, Instant Bitcoin/Blockchain Transactions

Transactions for the Future

Instant Payments. Lightning-fast blockchain payments without worrying about block confirmation times. Security is enforced by blockchain smart-contracts without creating a on-blockchain transaction for individual payments. Payment speed measured in milliseconds to seconds.

Scalability. Capable of millions to billions of transactions per second across the network. Capacity blows away legacy payment rails by many orders of magnitude. Attaching payment per action/click is now possible without custodians.

Low Cost. By transacting and settling off-blockchain, the Lightning Network allows for exceptionally low fees, which allows for emerging use cases such as instant micropayments.

The Bitcoin Lightning Network:
Scalable Off-Chain Instant Payments

Joseph Poon
joseph@lightning.network

Thaddeus Dryja
rx@awsomnet.org

January 14, 2016
DRAFT Version 0.5.9.2

Abstract

The bitcoin protocol can encompass the global financial transaction volume in all electronic payment systems today, without a single custodial third party holding funds or requiring participants to have anything more than a computer using a broadband connection. A decentralized system is proposed whereby transactions are sent over a network of micropayment channels (a.k.a. payment channels or transaction channels) whose transfer of value occurs off-blockchain. If Bitcoin transactions can be signed with a new sighash type that addresses malleability, these transfers may occur between untrusted parties along the transfer route by contracts which, in the event of uncooperative or hostile participants, are enforceable via broadcast over the bitcoin blockchain in the event of uncooperative or hostile participants, through a series of decrementing timelocks.

1 The Bitcoin Blockchain Scalability Problem

Lightning network

- Transacciones instantáneas.
- Comisiones realmente bajas.
- Software independiente, que requiere de comunicación con la blockchain de Bitcoin.
- LN puede integrarse en redes.

¿Por qué usar LN?

- Escalabilidad.
- Micropagos.
- Privacidad.
- Pagos instantáneos.

LN se plantea como una solución al problema de escalabilidad de Bitcoin. Aunque aún haya mucho por implementar y desarrollar.

116 Open Source Lightning Network Software Projects

Free and open source lightning network code projects including engines, APIs, generators, and tools.

Lnd 4633 ☆
Lightning Network Daemon ⚡

Lightning Rfc 1165 ☆
Lightning Network Specifications

Acinq Eclair 863 ☆
A scala implementation of the Lightning Network.

Lnbook 758 ☆
Mastering the Lightning Network (LN)

Lightninglabs Neutrino 531 ☆
Privacy-Preserving Bitcoin Light Client

Mixinnetwork Mixin 324 ☆
🚀 the Mixin TEE-BFT-DAG network reference implementation

Node Launcher 313 ☆
Easiest Bitcoin Lightning desktop app, for Windows, macOS, and Linux

Joule Extension 300 ☆
Lightning payments extension for Chrome

Rtl 297 ☆
Ride The Lightning - A full function web browser app for LND, C-Lightning and Eclair

Lightning Onion 279 ☆
Onion Routed Micropayments for the Lightning Network

Cyphernode 262 ☆
Modular Bitcoin full-node microservices API server architecture and utilities toolkit to build scalable, secure and featureful apps and services without trusted third parties

Jamaljsr Polar 236 ☆
One-click Bitcoin Lightning networks for local app development & testing

Pilares de Bitcoin

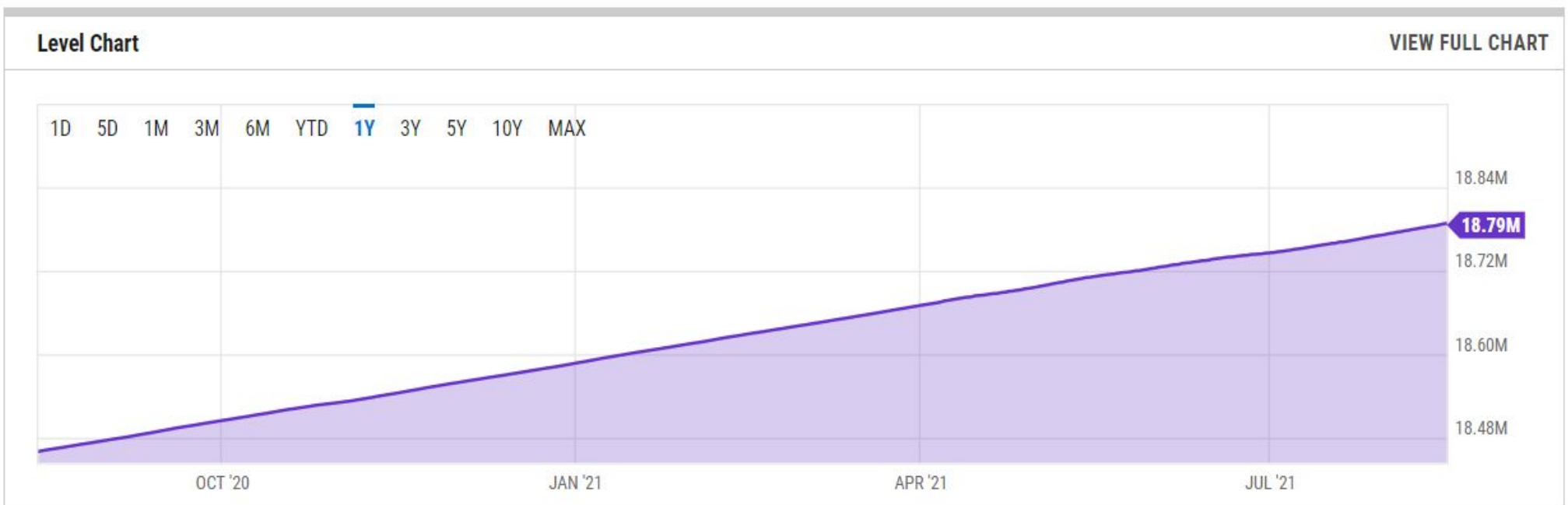
Abierto

Escaso

Bitcoin Supply

18.79M BTC for Aug 16 2021

Overview | Interactive Chart



Público

Explorador > Bitcoin Explorer

Buscar tu transacción, una dirección o un bloque

USD

Bitcoin

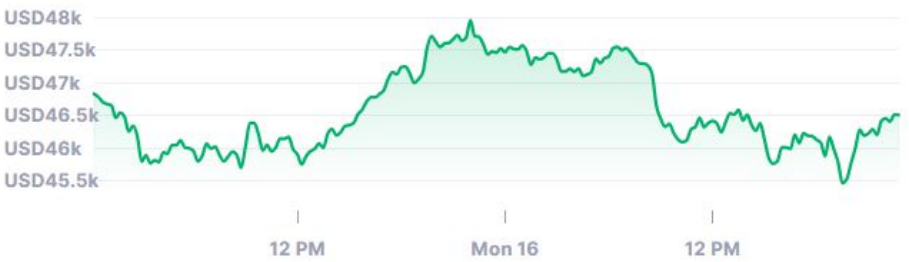
Información de Blockchain para Blockchain information for Bitcoin (BTC), incluyendo los precios históricos, los bloques minados más recientemente, el tamaño de mempool y la información de las últimas transacciones.

46.453,78 US$	119.861 EH/s	265,800	2.507m BTC	90,238 BTC
Precio →	Tasa de hash estimada →	Transacciones (24hrs) →	Volumen de transacciones →	Volumen de transacciones (Est) →

Precio

El precio de Bitcoin durante los últimos day

1 Day



Ver todos los precios →

Tamaño de mempool (Bytes)

El tamaño agregado de transacciones sin confirmar en bytes

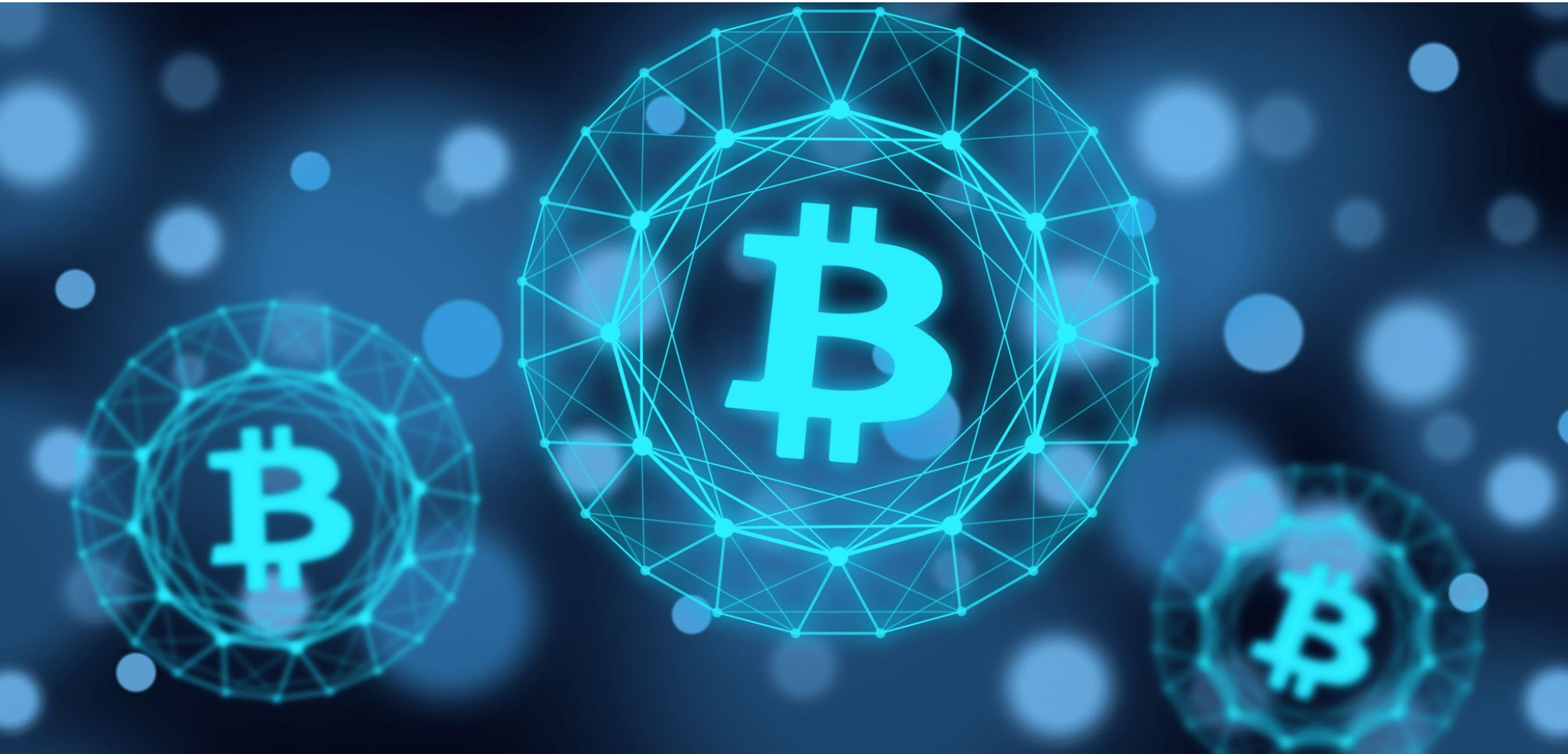
1 Day

Ver todos los gráficos →

Sin fronteras

Resistente a la censura

Descentralizado

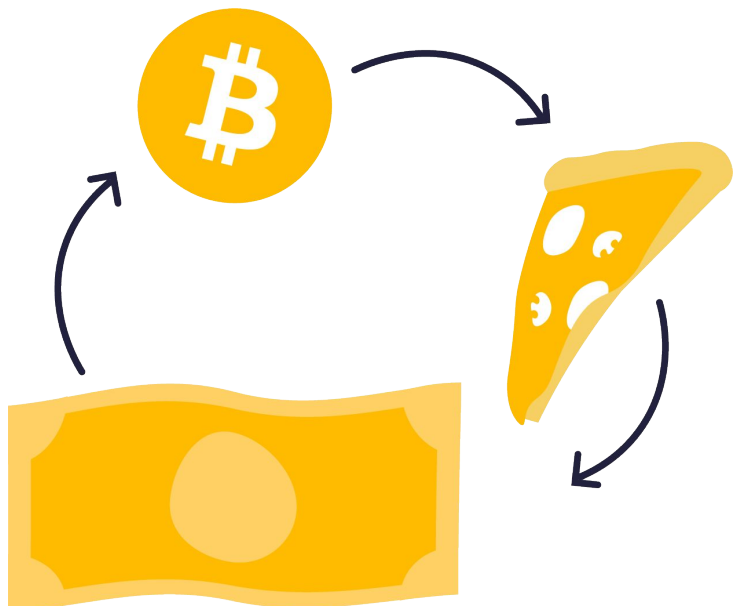


Confianza


Explorador
Crypto Prices
Bitcoin
Buscar token o activo
USD
Bitcoin BTC USD46,573.53
Comprar BTC
alizar operacion
24H
-USD2,467.70 (-1.64%)
Alto. USD47,735.50
Bajo: USD45,267.80
24H
1S
1M
1A
Todo
Personalizado
Aug 15, 2021
Aug 16, 2021
Línea
Gráficos de velas
80000.00
70000.00
60000.00
50000.00
46576.87
40000.00
30000.00
20000.00
10000.00
0.00
Jul 31
Dec 31
May 31
Dec 31
May 31
Dec 31
May 31
Dec 31
May 31
Dec 31
May 31

Usos de Bitcoin

- Dinero como primera aplicación.
- Pago de bienes y servicios.
- Envío de remesas.
- Intereses.
- Préstamos utilizando Bitcoin como garantía.
- Reserva de valor.



Blockchain más allá de Bitcoin

Más allá de Bitcoin

- Inmutabilidad
- Transparencia
- Trazabilidad

50+ BLOCKCHAIN
REAL WORLD USES CASES

GOVERNMENT
Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

essentia.one

IDENTIFICATION
Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport**.

uport

MOBILE PAYMENTS
The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

ripple

INSURANCE
A smart contract-based blockchain is being used by Insurer **American International Group Inc** as a means of saving costs and increasing transparency.

AIG

ENDANGERED SPECIES PROTECTION
The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.

CARBON OFFSETS
IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.

IBM HYPERLEDGER

ENTERPRISE
Ethereum's blockchain can be accessed as a cloud-based service courtesy of **Microsoft Azure.**

Microsoft Azure

BORDER CONTROL
Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.

essentia.one

SUPPLY CHAINS
IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.

IBM Walmart

HEALTHCARE
A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**

MEDREC

SHIPPING
Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.

MÆRSK

REAL ESTATE
Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by **Propy.**

PROPY

ENERGY
Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.

essentia.one

LAND REGISTRY
Land registry titles are now being stored on the blockchain in Georgia in a project developed by the **National Agency of Public Registry**.

NATIONAL AGENCY of PUBLIC REGISTRY

COMPUTATION
Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.

DIGITAL CURRENCY GROUP

ADVERTISING
New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.

NYIAX

BORDER CONTROL
Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.

essentia.one

JOURNALISM
Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as **Civil** has shown.

CIVIL

WASTE MANAGEMENT
Waltonchain is using **RFID** technology to store waste management data on the blockchain in China.

ENERGY
Food importation is another industry where blockchain is proving its worth, with **Louis Dreyfus Co** trialling a soybean importation operation using this technology.

LDC. Louis Dreyfus Company

DIAMONDS
The **De Beers Group** is using blockchain to track the importation and sale of diamonds.

DE BEERS GROUP OF COMPANIES

FINE ART
By storing **certificates** of authenticity on the blockchain, it's possible to dramatically reduce art forgeries, as one blockchain project is proving.

NATIONAL SECURITY
For the past two years, the **US Department of Homeland Security** has been using blockchain to record and safely store data captured from its security cameras.

TOURISM
In a bid to boost its tourism economy, **Hawaii** is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

TAXATION
In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network**.

ENERGY
Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.

CNE COMISIÓN NACIONAL DE ENERGÍA

RAILWAYS
Russian rail operator **Novotrans** is storing inventory data on a blockchain pertaining to repair requests and rolling stock

НОВОТРАНС

ENTERPRISE
Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by **Alphabet Inc**

Google Alphabet

MUSIC
Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

arbit

FISHING
Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

Propiedades y características

- Consenso distribuido.
- Transparencia y trazabilidad.
- Inmutabilidad.
- Descentralización.
- Longevidad.
- Transferencias rápidas.
- Costos transaccionales bajos.

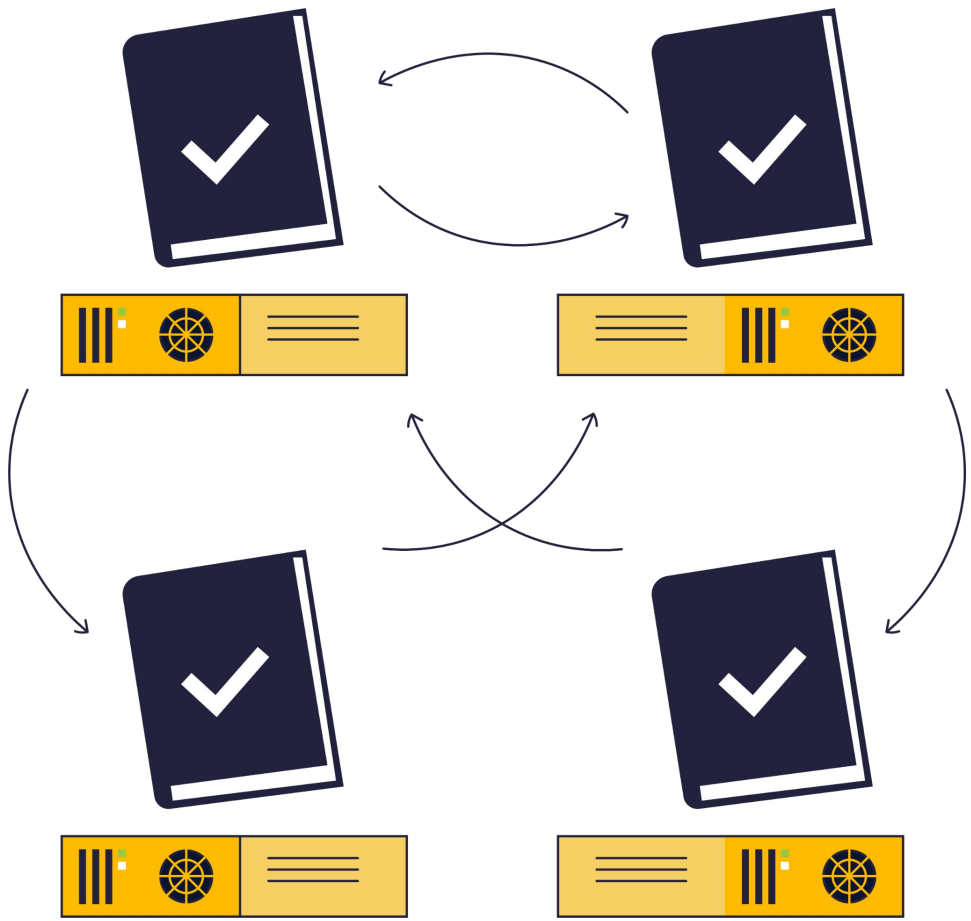
Cryptocurrency Category by 24h Price Change

We have created an index for each cryptocurrency category. Categories are ranked by 24h price change. Click on a crypto category name to see the constituent parts of the index and their recent price performance.

#	Name	Avg. Price Change	Top Gainers	Market Cap	Dominance	Volume	Gainers / Losers Number
1	Masternodes	▲ 21.79%	ION ION ▲ 2132.7%	$4,354,271,876 ▼ 2.06%	0.22%	$463,802,112 10,016 BTC	22 (19%) 92 (81%)
2	Tourism	▲ 19.31%	Tavittcoin TAVITT ▲ 106.17%	$148,132,233 ▲ 2.06%	0.01%	$7,992,149 173 BTC	5 (42%) 7 (58%)
3	Solana Ecosystem	▲ 15.18%	Moonlana MOLA ▲ 213.83%	$116,424,065,878 ▲ 4.1%	5.84%	$96,606,085,645 2,086,314 BTC	26 (65%) 14 (35%)
4	Music	▲ 10.34%	Audius AUDIO ▲ 115.63%	$1,408,290,240 ▲ 111.39%	0.07%	$827,466,855 17,870 BTC	4 (40%) 6 (60%)
5	Lending / Borrowing	▲ 9.83%	fyeth.finance YETH ▲ 337.78%	$15,306,702,619 ▼ 0.73%	0.77%	$1,818,831,633 39,280 BTC	15 (45%) 18 (55%)
6	Binance Labs Portfolio	▲ 7.09%	Audius AUDIO ▲ 115.63%	$1,273,352,847,283 ▼ 2.48%	63.89%	$60,451,948,287 1,305,526 BTC	7 (41%) 10 (59%)
7	Multicoin Capital Portfolio	▲ 6.91%	Audius AUDIO ▲ 115.63%	$1,353,054,549,226 ▼ 2.08%	67.88%	$64,278,992,736 1,388,175 BTC	9 (47%) 10 (53%)
8	Interoperability	▲ 5.41%	SonoCoin SONO ▲ 136.76%	$7,745,250,652 ▼ 0.33%	0.39%	$667,695,086 14,420 BTC	14 (48%) 15 (52%)
9	PetRock Capital	▲ 5.09%	TeraBlock TBC ▲ 71.54%	$522,666,015 ▼ 34.61%	0.03%	$293,707,293 6,343 BTC	10 (48%) 11 (52%)
10	Heco Ecosystem	▲ 5.03%	Dogeswap DOGES ▲ 42.02%	$2,905,627,701 ▼ 0.13%	0.15%	$121,198,259 2,617 BTC	14 (56%) 11 (44%)

Tipos de Blockchain

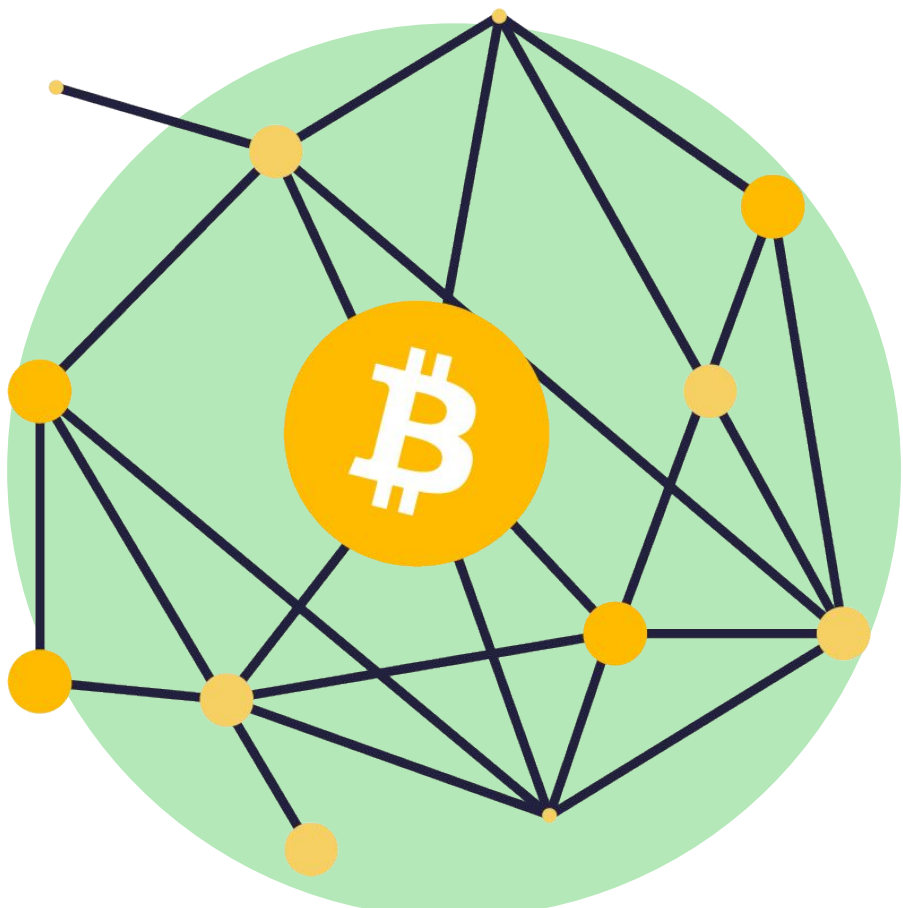
- Públicas
- Privadas
- Híbridas



Públicas

Accesible a cualquier persona del mundo.

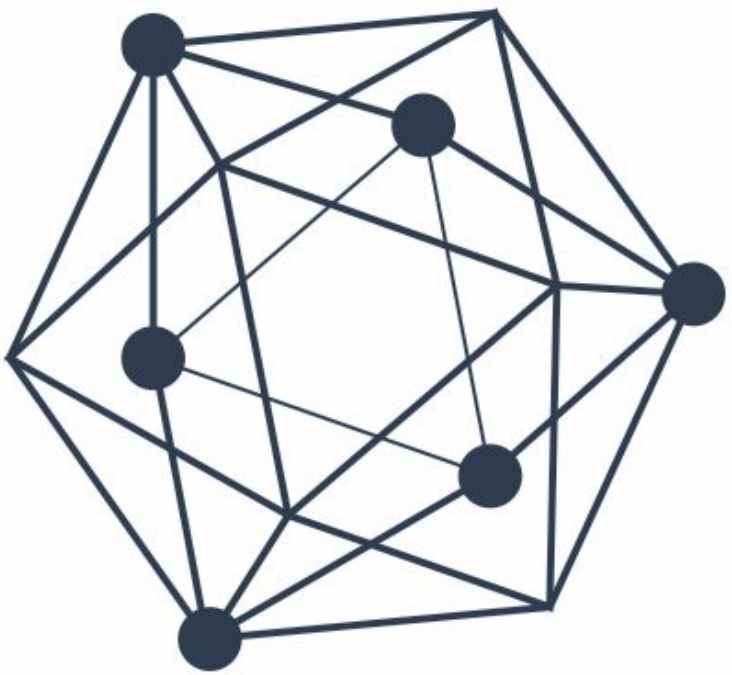
Ejemplo: Bitcoin, Ethereum, etc.



Privadas

Válidas para solventar problemas de eficiencia, seguridad y fraude dentro de instituciones financieras tradicionales.

Ejemplo: Hyperledger, etc.



Híbridas

Intento de aprovechar lo mejor de ambos mundos. La participación en la red es privada pero la contabilidad es accesible de forma pública.

Ejemplo: R3, Energy Web, etc.

Evolución de Blockchain

- Blockchain 1.0: Digital Currency
- Blockchain 2.0: Smart Contracts
- Blockchain 3.0: DApps
- Blockchain 4.0: Industry

Blockchain 1.0

Digital Currency

Blockchain 1.0

Es la primera fase de evolución en el desarrollo de esta tecnología.

Se derivó de la estructura original de Bitcoin, que a su vez tomó conceptos e ideas de proyectos que iniciaron en la era cypherpunk.

Tecnologías

Blockchain mostró el potencial de interrumpir innumerables industrias; sin embargo el desarrollo blockchain se centró en la creación de criptomonedas.

- DLT (Tecnología de registro distribuido)
- Blockchain
- PoW

Objetivos

- Crear una nueva forma revolucionaria de abordar las finanzas.
- Brindar transparencia a través de un sistema de registro de transacciones distribuido e inmutable.
- Acceso público al sistema financiero global.

Blockchain 2.0

Smart Contracts

Blockchain 2.0

Facilita el intercambio de valor más allá de bitcoin y las criptomonedas, mediante los contratos inteligentes.

El registro de información no está directamente relacionado con dinero, sino que se almacena cualquier otro tipo de archivo o activo digital.

Tecnologías

Está pensado para la gestión y transferencia de activos y cualquier otro tipo de bien que pueda estar en un registro público.

- Smart Contracts
- Ethereum Virtual Machine (EVM)

Objetivos

- Ejecuta de forma automática acciones programadas en blockchain.
- Registro y transferencia de valor más allá del dinero.
- Autonomía, nuevos modelos de negocio, anonimato.

Blockchain 3.0

DApps

Blockchain 3.0

Se introdujo para abordar problemas como:

- Escalabilidad
- Sostenibilidad
- Seguridad
- Costo
- Dilemas de interoperabilidad

Redes blockchain programables, capaces de soportar **aplicaciones descentralizadas**, con mucha mayor capacidad que Bitcoin y Ethereum.

Tecnologías

Escalables, con una interfaz amigable para los usuarios y eficientes.

- Proof of Stake (PoS), Proof of History (PoH), etc.
- DApps (IPFS)

Objetivos

- Ejecuta de forma automática acciones programadas en blockchain.
- Registro y transferencia de valor más allá del dinero.
- Autonomía, nuevos modelos de negocio, anonimato.
- Escalabilidad.

Blockchain 4.0

Industry

Blockchain 4.0

Es una solución idónea para hacer más eficientes los entornos industriales.

Se presenta como apuesta firme para empresas. La industria 4.0 se vislumbra como una industria más segura, controlada, flexible y eficiente, gracias a las ventajas que otorga Blockchain.

Tecnologías

Trazabilidad de cadena de valor de suministro y la gestión de los objetos de internet de las cosas.

- IoT.
- Smart Contracts.
- Blockchain.

Objetivos

- Mejorar procesos existentes e impactar para modificar la producción de bienes.
- Cambiar las relaciones entre diferentes empresas.
- El cliente final verá cambios en la forma en que recibe productos y servicios.

Protocolos de Consenso

Protocolos de consenso

Es el mecanismo que regula la forma en que los nodos crean los bloques llegando a un acuerdo entre sí para poder hacerlo e incorporar ese bloque a la cadena.

Existen diferentes algoritmos de consenso, la selección del algoritmo depende en gran medida del tipo de aplicación que se quiera implementar.

Proof of Work

Los mineros ponen sus equipos a trabajar en resolver un acertijo criptográfico (hash). A mayor capacidad de cómputo mayor la probabilidad de resolver el acertijo.

Proof of Work

Desventajas:

- Altos costos de energía.
- Vulnerabilidad al ataque del 51%.

Proof of Stake

En lugar de mineros gastando energía para recibir una recompensa por minar bloques, en **PoS** los nodos “validadores” deben invertir una cantidad de criptomoneda.

PoS elige de forma aleatoria al nodo validador que agrega el próximo bloque a la cadena.

Funciona como una lotería.

Proof of Stake

Ventajas:

- Velocidad.
- Eficiencia (Consume menos energía).
- Menos hardware.

Desventajas:

- Vulnerabilidad.
- Concentración de riqueza.

Otros

- Delegated Proof of Stake (DPoS)
- Proof of History (PoH)
- Proof of Elapsed time (PoET)
- Practical Byzantine Fault Tolerance (PBFT)
- Proof of Humanity (PoH)

Limitaciones de Blockchain

Limitaciones de Blockchain

- Inmutabilidad de la información.
- Velocidad de procesamiento de información.
- Imposibilidad de recuperar accesos.
- Ataque del 51%.
- Escalabilidad.
- Privacidad.

Futuro de Blockchain