

Más allá del 12 de mayo de 2017



Yaiza Rubio Viñuela
(@yrubiosecc | yaiza.rubio@11paths.com)



Wana Decrypt0r 2.0



Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

About bitcoin

How to buy bitcoins?

Contact Us

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

 **bitcoin**
ACCEPTED HERE

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw619p7AA8isjr6SMw

Copy

Check Payment

Decrypt

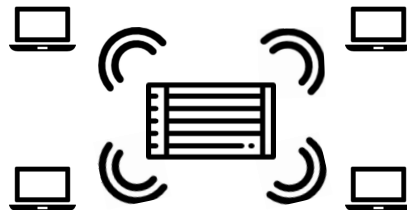
Cómo funciona la cadena de bloques (de Bitcoin)



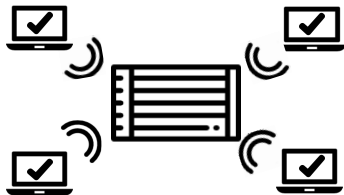
A quiere mandar *bitcoins* a B.



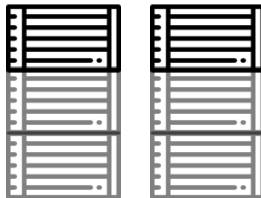
Alicia creará una transacción **firmándola** con su clave privada.



La información de la transacción es **notificada** al resto de nodos de la red.



Tras validarla, uno de los nodos será el encargado de **añadirla** en un **nuevo bloque** a la blockchain.



Los bloques encadenados se **replicarán** entonces en el resto de nodos de la red.



B podrá hacer uso de los *bitcoins* recibidos de **A**.

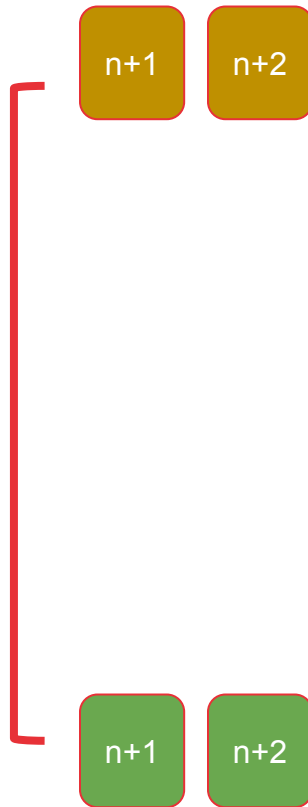
Los hard forks

**Durante 8 años hubo consenso
sobre las reglas que debían
regular el ecosistema de Bitcoin**



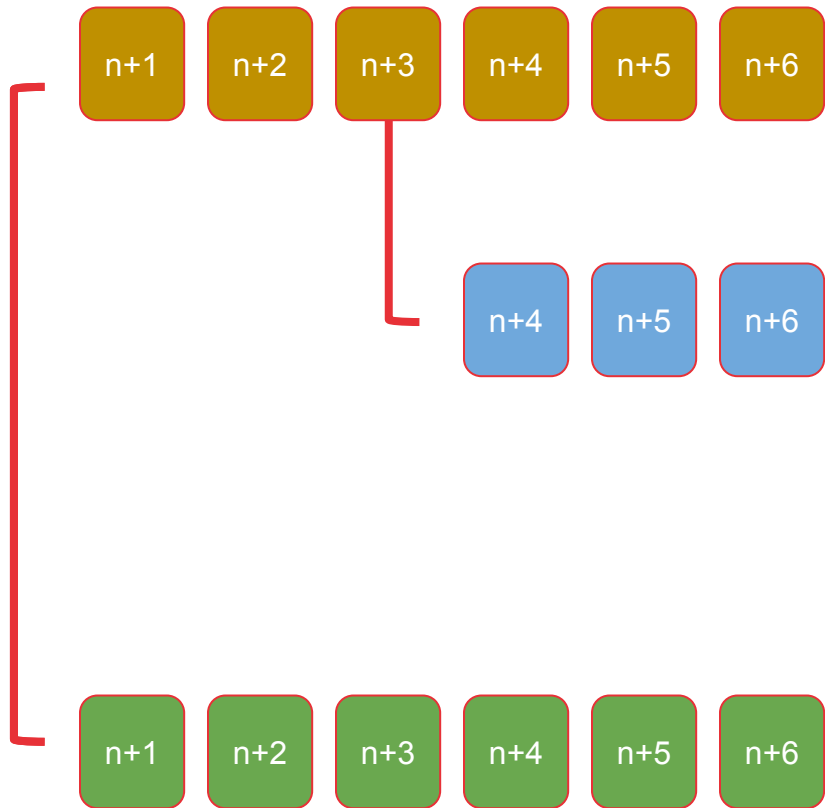
Los hard forks

**Durante 8 años hubo consenso
sobre las reglas que debían
regular el ecosistema de Bitcoin**



Los hard forks

**Durante 8 años hubo consenso
sobre las reglas que debían
regular el ecosistema de Bitcoin**

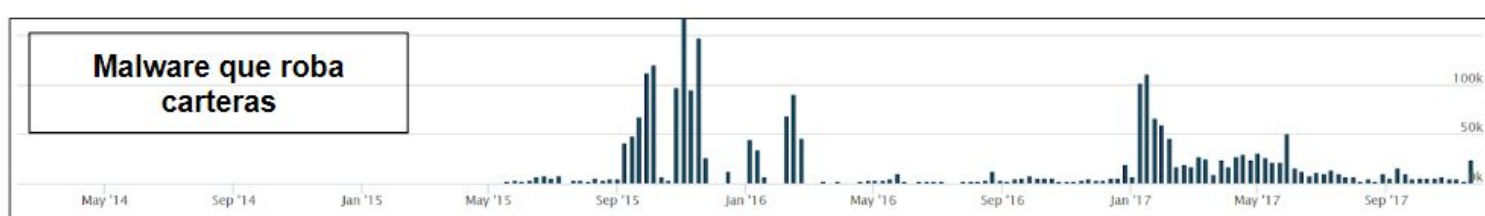


Tipos de ataques a los monederos



 bitaddress.org

Tipos de ataques a los monederos



CRITICAL WARNING

Nov 26, 2017 | Uncategorized

Bitcoin GOLD

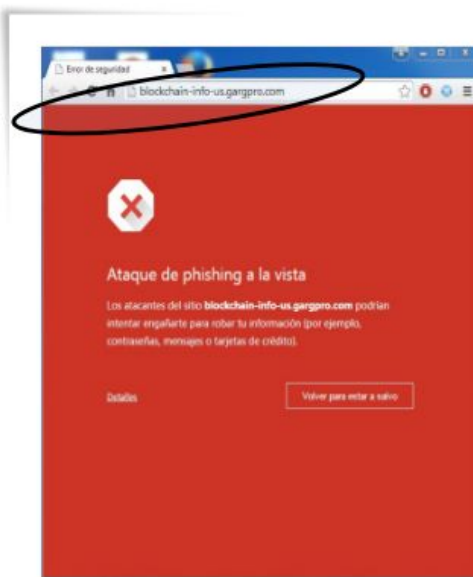
Updated: Sunday, November 26, 2017, 17:00 UTC

NOTE: We have expanded the recall window for the Windows Wallet Installer. Carefully note the expanded times/dates indicated below. The files currently available on Github through our web site are correct; always check the SHA-256 checksum against your downloaded files.

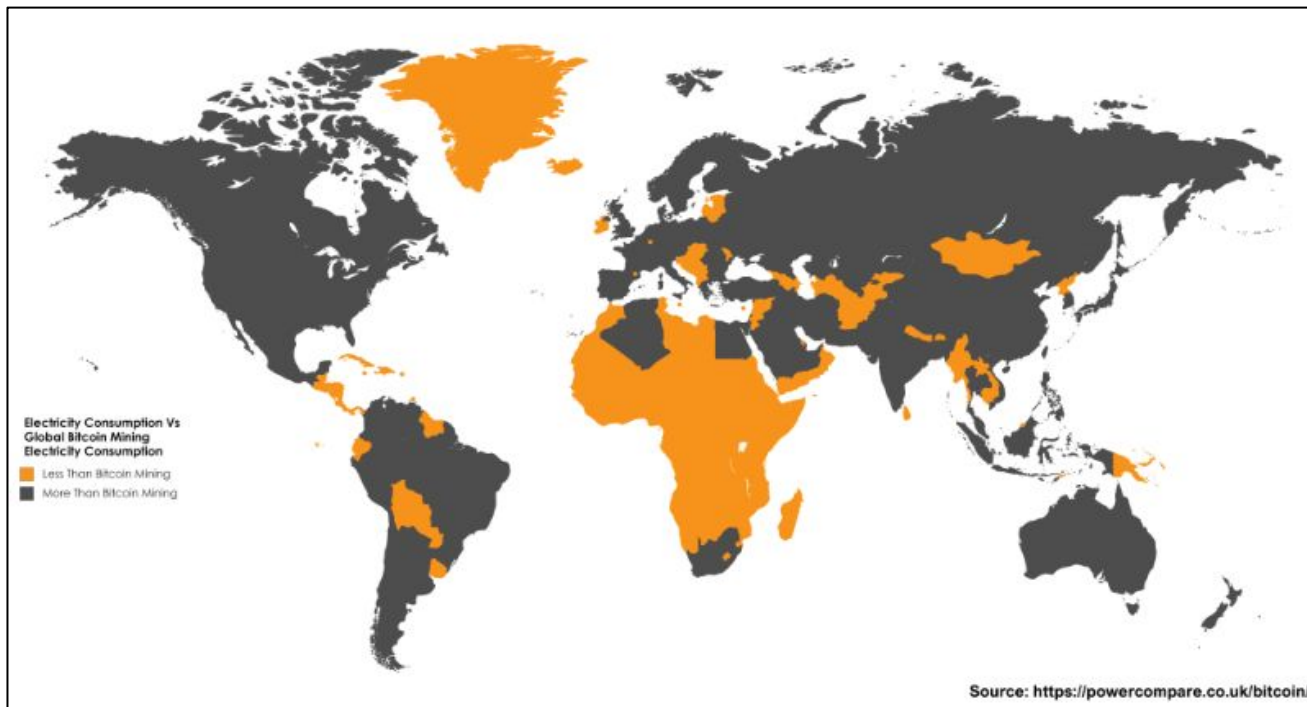
Please be aware that for approximately 4.5 days, a link on our Download page and the file downloads on our Github release page have been serving two suspicious files of unknown origin.

Until we know otherwise, all users should **presume these files were created with malicious intent** - to steal cryptocurrencies and/or user information. The file does not trigger antivirus / anti-malware software, but do not presume the file is safe.

Any user who verified the SHA-256 checksum of the download against the checksum listed on our Download pages is already aware the file is not authentic and should not have used the file, but nobody should assume that all users take this important step.



Regiones con menor consumo energético anual que la red de Bitcoin



¿Y si nos ahorramos la energía?

El malware que se dedica a la minería no es reciente aprovechando que el atacante no paga esa electricidad.

Ha habido diferentes familias que han implementado funcionalidades diferentes.

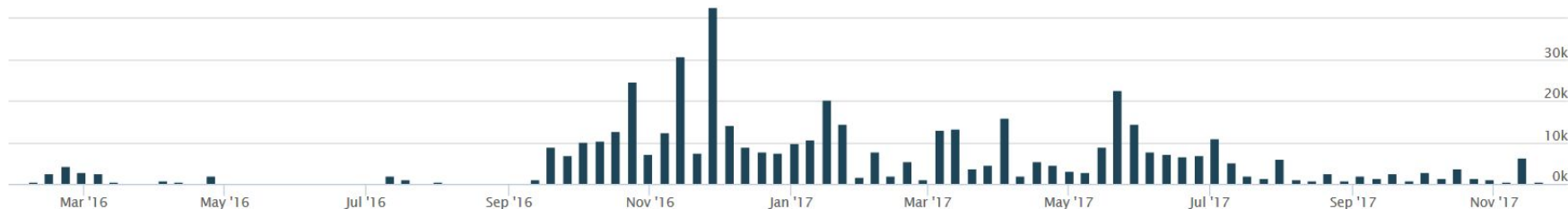
Photominer

MoneroMiner

MinerGate

DiscordiaMiner

CoinMiner

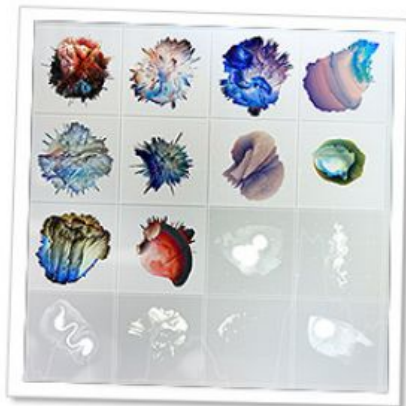


¿Y si nos ahorramos la energía?

October's Most Wanted Malware: Cryptocurrency Mining Presents New Threat

by Check Point Research Team

posted 2017/11/13



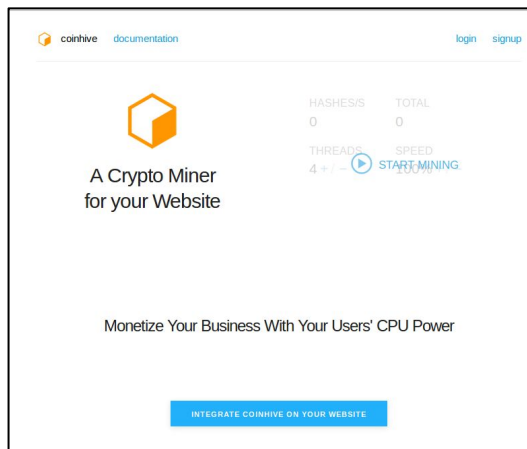
Check Point's latest Global Threat Index has revealed crypto miners were an increasingly prevalent form of malware during October as organizations were targeted with the CoinHive variant

Crypto **mining** is emerging as a silent, yet significant, actor in the threat landscape, allowing threat actors to extract substantial profits while victims' endpoints and networks suffer from latency and decreased performance. The emergence of Seamless and CoinHive once again highlights the breadth and depth of the challenges organizations face in securing their networks against cyber-criminals.

Following up on recent Check Point **research that found** that cryptocurrency miners can use up to 65% of an end users total CPU, the CoinHive variant entered the Index in 6th place last month. Without the user knowing or approving, the malware mines the Monero cryptocurrency whenever a user visits a web page. CoinHive is implanted via JavaScript, which then uses high levels of the end-users CPU and severely impacts the machine's performance.

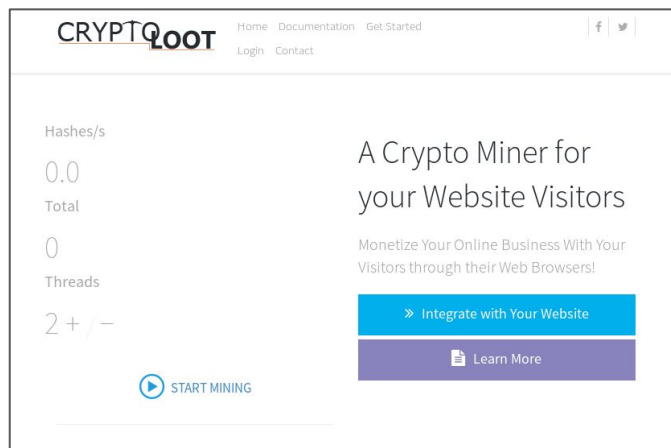
¿Una nueva forma de financiación?

Existen proyectos destinados a cargar Javascript de minado de Monero que se ejecutan mientras el usuario visita una web



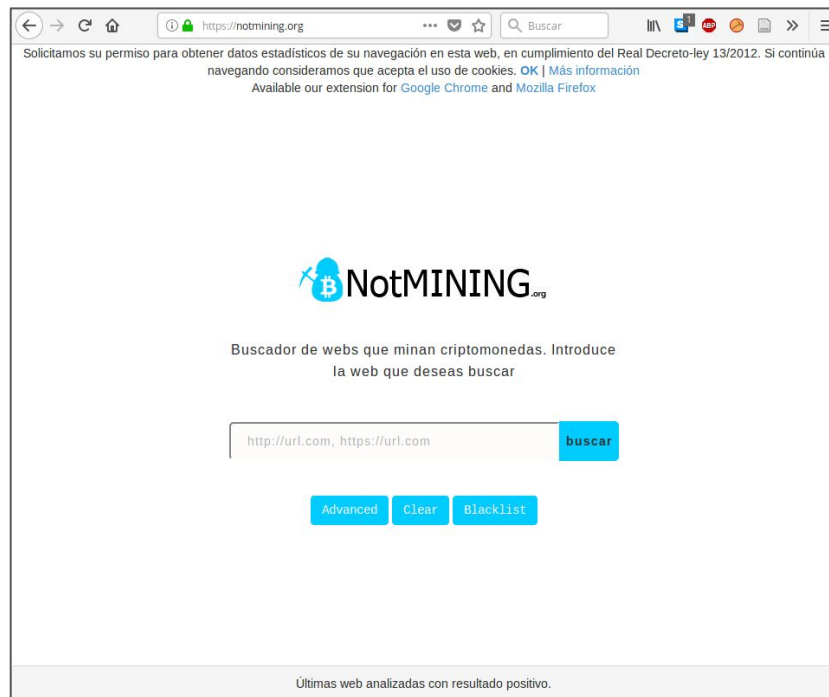
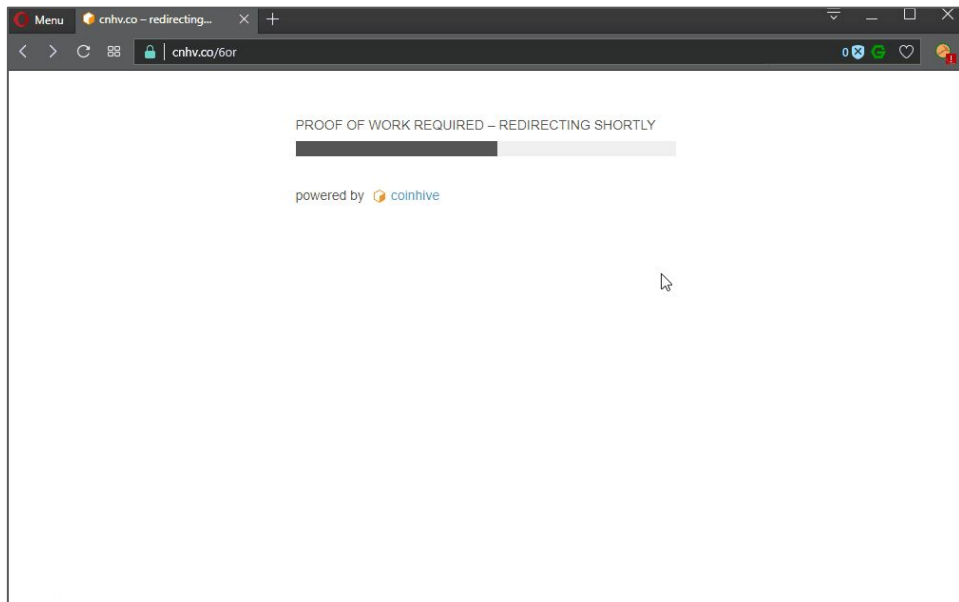
coinhive.min.js
056914e579e9ecb82809850f5eff8265
30% de comisión
<https://coinhive.com/lib/coinhive.min.js>

miner.min.js
c0ee8328586ed8f4ee2ef954a28128aa
12% de comisión
<https://crypto-loot.com/lib/miner.min.js>



Pero, ¿podemos protegernos?

Extensiones como No Coin bloquean las conexiones a sitios asociados con prácticas de minería disponible para Firefox y Google Chrome mientras que Opera ya integra esta protección por defecto.



<https://github.com/keraf/NoCoin> | <https://notmining.org>

Malware que monitoriza el clipboard

Qutra
me/Qutrachka | Project
Evrial

PROJECT
QUTRA
EVRIAL

posts
5 sympathies
month with us

Login or register to view links

Spoiler: How the product works

1. The victim launches the EXE (Which is being rebuilt in the web panel, which is activated by you after purchasing the product). It is written to the startup (Each time the PC starts, it launches the password stylus / cookie and the clipper operation).
2. Project Evrial expects any change to the clipboard, and if it determines that the clipboard contains a supported format, makes a request for a secure web connection to the web panel, gets what it needs to replace and makes a replacement.
3. The Web panel displays that the clipboard has changed.
4. Despite waiting for the change of the clipboard, a .zip file from the stylus is sent to the web panel (Desktop screen, desktop files, passwords, cookies) and it is also displayed in it.

Spoiler: Programs supported stylists | Replacing wallets

Clipper:

BTC, LTC, MONERO, ETHEREUM
QIWI, WMR, WMZ, WME.
Steam Trade Offer Link

Stealer:

Supported browsers:

Chromium (Passwords + Cookies)
Google Chrome (Passwords + Cookies)
Opera (Passwords + Cookies)
Kometa (Passwords + Cookies)
Amigo (Passwords + Cookies)
Orbitum (Passwords + Cookies)
Orbitum (Passwords + Cookies) , the cookies have)
Comodo Dragon (+ Passwords, the cookies have)
Yandex Browser (Passwords, the cookies have +)

Supported utilities:

CryptoClipWatcher, our new tool against crypto clipboard hijacking techniques

📅 tuesday, july 17, 2018

Since 2017, this technique is becoming quite popular. Cryptocurrency in general is a new target for malware, and mining Bitcoins is not profitable anymore in regular computers (maybe Monero is). But, targeting the clipboard to steal cryptocurrency is a new, easy and interesting way that malware creators are exploiting. We have created a simple tool that watches your clipboard to alert you if the destination cryptocurrency address changes.





¿Cómo almacenamos
información?

Los inicios sobre el almacenamiento

Anteriormente, para almacenar información en la cadena de bloques se enviaba dinero a direcciones de Bitcoin que eran válidas pero cuya clave pública era generada arbitrariamente y no a partir de una clave privada. De esta manera, si se envían pequeñas cantidades de moneda a estas direcciones se sabe que NO se van a poder gastar, pero se puede utilizar este *hack* para **incrustar en la parte pública de una dirección información** que quedará registrada de forma permanente en la blockchain como información real.

Ejemplos hay muchos, veamos la siguiente transacción:

<https://blockchain.info/tx/8881a937a437ff6ce83be3a89d77ea88ee12315f37f7ef0dd3742c30eef92dba>

El ejercicio consiste en:

1. Buscar una dirección que comiende por 15g
2. Verificar si esa dirección es válida: <http://lenschulwitz.com/base58>
3. Decodificar la dirección de Base58 a hexadecimal
4. Decodificar esa información en hexadecimal a caracteres ASCII. **¿Qué obtenemos?**

¿Qué es OP_RETURN?

Es una funcionalidad incorporada en 2013 con el objetivo de **almacenar** una pequeña parte de **información** (80 bytes) en la cadena de bloques.

```
> bitcoind getrawtransaction 8bae12b5f4c088d940733dcd1455efc6a3a69cf9340e17a981286d3778615684 1
```

```
>>> deserialize(d)
```

```
{
  "inputs": [
    {
      "address": "1HnhWpkMHMjgt167kvgcPyrMmsCQ2WPgg",
      ...
    }
  ],
  "outputs": [
    {
      "address": "j\u0013charley loves heidi",
      "prevout_n": 0,
      "scriptPubKey": "6a13636861726c6579206c6f766573206865696469",
      "type": 2,
      "value": 0
    },
    {
      "address": "1HnhWpkMHMjgt167kvgcPyrMmsCQ2WPgg",
      "prevout_n": 1,
      "scriptPubKey": "76a914b8268ce4d481413c4e848ff353cd16104291c45b88ac",
      "type": 0,
      "value": 200000
    }
  ],
  "version": 1
}
```

```
"scriptPubKey" : {
  "asm" : "OP_RETURN 636861726c6579206c6f766573206865696469",
  "hex" : "6a13636861726c6579206c6f766573206865696469",
  "type" : "nulldata"
}
```

Hex to ASCII converter

Enter 2 digits hex numbers with any prefix / postfix / delimiter and press the Convert button:

636861726c6579206c6f766573206865696469

Convert Reset

charley loves heidi

¿Qué es OP_RETURN?

Coin Secrets beta

Testnet Mainnet

Recent Metadata in the Bitcoin Blockchain

Below is a list of metadata recently embedded in the bitcoin blockchain using [OP_RETURN](#) outputs.

This method was made official in [Bitcoin 0.9](#) due to [user demand](#). Opinions [differ strongly](#) and the [future is open](#).

Also from Coin Sciences: [MultiChain for private blockchains](#) with full compatibility with Bitcoin Core.

More on OP_RETURN: [CoinSpark protocol](#) – [Bitcoin 2.0 presentation](#) – [PHP](#) and [Python](#) libraries.

Block	Transaction ID	OP_RETURN metadata
[new]	1d7c8881c39b694779eb4a0b147c376e8703b77d0c1c3d88c2840ae76a9103 biteasy blockexplorer blockr blocktrail	<pre>???[is\$Rd3\$StR???1?+]?:?y?Kuq?Tf3???6?@?S?d????R???suJA?????jw+8v5m6BDTfVvUPcEKUmQzEIN0Uh+NCQkxZldBO46qXmIS3Vx+VRmYDP8xY240CPU4lksMLDz+VSI4LOc3VdQf7fMtS6n13Kw== (base64)6a49f2fe66e810d3ad5b8f73f124526433125374521f8d090931ce2b5d04ee3aa979a54b7571f954666033fcdf1636e3408f538964b0c2c3cfe5529782f473755d41fed9ad4ceea7d772b (raw)</pre>
[new]	4916e3472773bc7e18d306069c0bf418c6c602ca4960507435634c1aef107 biteasy blockexplorer blockr blocktrail	<pre>S6?[-???????????q?8????A??>??F\$Uza6fC0qpYaN8q/5kMGNIpFXDjYKQORuEHV7CDG/T7B2EYk (base64)6a245336ba7c2d2aa5868d72aff990c18d88f1710e38d8910391b841d5ec20c6fd3ec1d84624 (raw)</pre>
[new]	5c41a18194d6db486f19941d16ce4a2bd88a83d7d6201486538623c34b79ab16 biteasy blockexplorer blockr blocktrail	<pre>GCHNs<???g?????6?_?A???~?S?^?????TIRONITnM83hnpZ6arFebvOjYdX6Zc9r6f8fhsU+de4uOT18dUbA== (base64)6a254743484e733cde19e967a6ab15e6d53a361d5fa65cf6bec7e182c53e75ee2ed13d7c7546c (raw)</pre>

En proyectos como [coinsecrets.org](#) se enumeran los mensajes que se incluyen en las distintas transacciones registradas en la cadena de bloques de Bitcoin.

BLOCKCHAIN

MONEDERO GRÁFICAS ESTADÍSTICAS MERCADOS API

🔍 Buscar hash de bloque, transacción, dirección, etc.

Transacción

Ver información de una transacción de Bitcoin

1d7c8881c39b694779eb4a0b147c376e8703b77d0c1c3d88c2840ae76a9103

12V4qP7ZaWYyqZqZf358K4uB8A79aC5 (0.0058588 BTC - Producción)

➡ No es posible decodificar la dirección de salida - (No gastado)

12V4qP7ZaWYyqZqZf358K4uB8A79aC5 - (No gastado)

0.0058588 BTC

0.0004838 BTC

Transacción en Confirmar

0.0004838 BTC

Resumen

Entradas y Salidas

tamaño276 (bytes)

total de entrada0.0058588 BTC

Hora de Recepción2017-06-21 09:00:44

Salida Total0.0004838 BTC

Retransmitido por la IP95.130.254.151 (whoiis)

Comisiones0.00080753 BTC

VisualizarVer Grafico de Artor

Tarifa por byte292.583 sat/B

Estimado de BTCs transaccionados0 BTC

ScriptsCoular scripts y Coinbase

¿Cómo almacenamos muchos datos?

Guardando *punteros* que se apoyen en otras tecnologías que también garanticen la **descentralización**.

Apoyándonos en IPFS, una tecnología P2P que se ha ganado fama últimamente tras ser utilizada por los organizadores del referéndum el 1 de octubre para evitar la censura.



Página archiadas en archive.org en:

<https://web.archive.org/web/20170923080326/https://gateway.ipfs.io/ipns/QmZxWEBJB/VkGDGaKdYPQUXX4KC5TCWbvur4iYZrTML8XCR/>

EP | Madrid 23/09/2017 - 09:49 h. CEST

El presidente de la Generalitat, Carles Puigdemont, ha difundido este sábado un nuevo enlace de Internet para consultar dónde puede votar cada catalán en el referéndum ilegal del **1 de octubre**.



Lo ha hecho después que el Tribunal Superior de Justicia de Cataluña (TSJC) ha instado este viernes a la Guardia Civil a deshabilitar el acceso a la página web onvotar.garantiespelreferendum.com, que ya ha sido cerrada.

Este dominio ha sido intervenido y se encuentra a disposición de la Autoridad Judicial



This domain name has been seized pursuant to a seizure warrant under the Judicial Authority and is under its administration

Mensaje que aparece al intentar entrar en el enlace que este viernes cerró la Guardia Civil. / Cadena Ser

"No se pueden poner puertas al campo: en esta web encontrarás el lugar en el que te corresponde votar el 1 de octubre:

<https://gateway.ipfs.io/ipns/QmZxWEBJB/VkGDGaKdYPQUXX4KC5TCWbvur4iYZrTML8XCR/#1Oct>", ha escrito en un mensaje en Twitter, que ha sido rápidamente compartido por usuarios en redes.



Tendencias hacia
el anonimato total

Tendencias en anonimato



Mientras que en Bitcoin el saldo de una cuenta es público, existen otras criptodivisas que protegen esa identidad. Monero utiliza firmas en anillo para enmascarar origen, destinatario y saldo de las transacciones.

<http://getmonero.org/>



Zcash es un protocolo creado en 2016 con el objetivo de facilitar. Los usuarios pueden (opcionalmente) usar zk-Snarks para enmascarar el emisor, receptor y saldo de una transacción.

<https://z.cash/>



Basada en el código fuente de Bitcoin, Dash surge en 2014. Cuenta con dos tipos de nodos: *nodes* (mineros) y *masternodes* (a cargo de la gobernanza y de usos extra como los envíos instantáneos y anónimos).

<https://www.dash.org/>



2018: ¡Boom de Blockchain!

Cómo funciona la cadena de bloques (de Bitcoin)



A quiere mandar *bitcoins* a B.

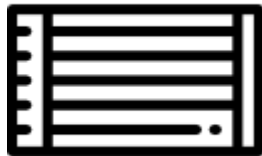
¿La dirección es un dato de carácter personal?

¿Los usuarios están preparados para tener direcciones y claves privadas?

Cómo funciona la cadena de bloques (de Bitcoin)



A quiere mandar *bitcoins* a B.



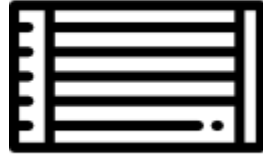
Alicia creará una transacción
firmándola con su clave privada.

¿Cómo dimensionamos los costes por transacción para un determinado servicio?

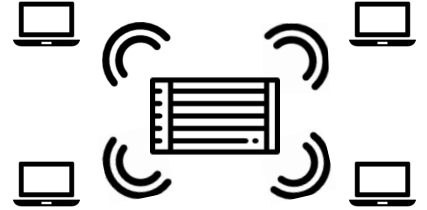
Cómo funciona la cadena de bloques (de Bitcoin)



A quiere mandar *bitcoins* a B.



Alicia creará una transacción
firmándola con su clave privada.



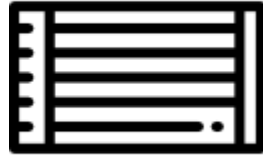
La información de la transacción es
notificada al resto de nodos de la red.

¿Cuántos nodos son necesarios para que
tenga sentido la descentralización?

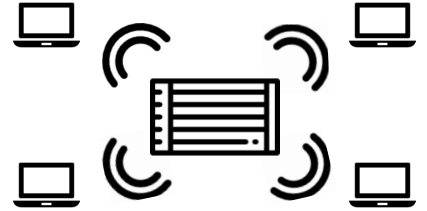
Cómo funciona la cadena de bloques (de Bitcoin)



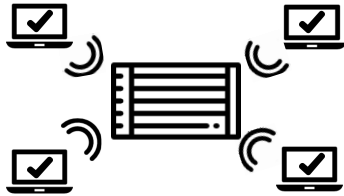
A quiere mandar *bitcoins* a B.



Alicia creará una transacción **firmándola** con su clave privada.



La información de la transacción es **notificada** al resto de nodos de la red.



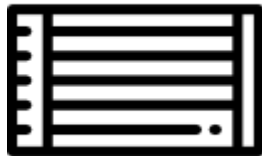
Tras validarla, uno de los nodos será el encargado de **añadirla** en un **nuevo bloque** a la blockchain.

¿Qué algoritmo de consenso es necesario? ¿Tiempos medios de confirmación

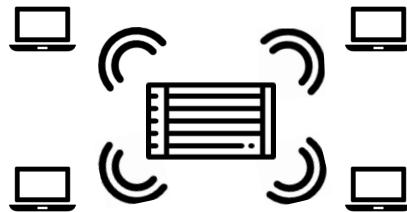
Cómo funciona la cadena de bloques (de Bitcoin)



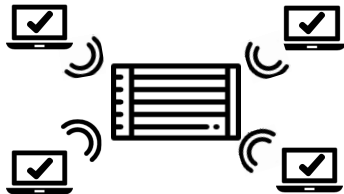
A quiere mandar *bitcoins* a B.



Alicia creará una transacción
firmándola con su clave privada.



La información de la transacción es
notificada al resto de nodos de la red.



Tras validarla, uno de los nodos será el encargado de **añadirla** en un **nuevo bloque** a la blockchain.



Los bloques
encadenados se
replicarán
entonces en el
resto de nodos de
la red.

¿Queremos que
todos los actores
vean la información
que circula?

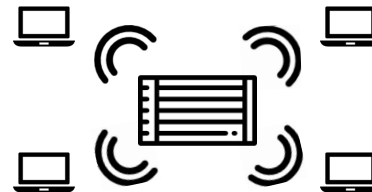
Cómo funciona la cadena de bloques (de Bitcoin)



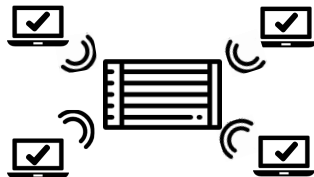
A quiere mandar *bitcoins* a B.



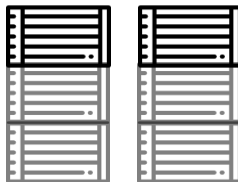
Alicia creará una transacción
firmandola con su clave privada.



La información de la transacción es
notificada al resto de nodos de la red.



Tras validarla, uno de los nodos será el encargado
de **añadirla** en un **nuevo bloque** a la blockchain.



Los bloques
encadenados se
replicarán
entonces en el
resto de nodos
de la red.



B podrá hacer uso de los
bitcoins recibidos de A.

¿Assets nativos en la cadena de bloques?

Deposit Funds

RIPPLE BTC EU BANK BANK ETH ETC REP QAU DASH

Use the following **Ethereum Classic** address to deposit funds:

Your deposit will take about one hour to complete.

Do not send any unsupported currency or token to this address! Currencies and tokens not supported by GateHub will **NOT** be credited and you will not be able to access them.

[Crosschain Recovery Policy](#)

0xfd17e762b62b3fd86f6255e5295f3fe9eb2012b4



Minimum deposit 0.100000 ETC



En un escenario convencional los usuarios tienen cuentas que gestionan ellos

Su problema es que el registro de todas las operaciones realizadas perdurará en la cadena de bloques.

El derecho al olvido en la RGPD: estándar CRUD

Artículo 17

Derecho de supresión («el derecho al olvido»)

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

- a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
- b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
- c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
- d) los datos personales hayan sido tratados ilícitamente;
- e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;
- f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

Más allá del 12 de mayo de 2017



Yaiza Rubio Viñuela
(@yrubiosecc | yaiza.rubio@11paths.com)