

Bitcoin y otras cripto-monedas



Capítulo estudiantil – Cinvestav Guadalajara IEEE Computer Society

- ¿Qué es?
 - Somos una asociación estudiantil sin fines de lucro orientada a la divulgación científica y tecnológica, con un enfoque particular en las ciencias computacionales.
- Misión
 - Nuestra misión es aportar a la divulgación de las ciencias computacionales, y la tecnología que deriva de ellas, para contribuir a la mejora de nuestro entorno y despertar el interés en estas áreas en la sociedad.
- Para saber más: <http://www.csgdl.org/>

Ciclo de Charlas de Cultura Computacional

- El ciclo de charlas de cultura computacional (C⁴) es una iniciativa del Capítulo Estudiantil de la IEEE Computer Society para tratar de divulgar temas del ámbito de las ciencias y tecnologías computacionales de una manera sencilla para las personas que no necesariamente entienden los tecnicismos del área en la que nos desarrollamos. Pretende ser un evento recurrente y exponer temas de actualidad y relevancia.
- <http://www.csgdl.org/portal/c4>

Expositor invitado

- Mtro. Erick Castellanos
 - Presidente del capítulo estudiantil.
 - Estudiante de doctorado en ciencias computacionales.
 - Tesis sobre vida artificial (en particular vida vegetal artificial).
 - Emprendedor.
 - Ideas XT – Soluciones de IT - <http://www.ideasxt.mx/>
 - Startup: Vevsi (tecnología educativa).

Patrocinadores

¡Agradecemos a la Rama Estudiantil del Cinvestav Unidad Guadalajara por su apoyo!

<http://www.ieeecinvestavgdl.mx/>

Bitcoin y otras cripto-monedas



Bitcoin

- ¿Qué es?
 - Divisa descentralizada, anónima y digital.
 - Protocolo.
 - Red P2P



Bitcoin

- Desarrollada en 2008 por “Satoshi Nakamoto”.
- Publicada en un artículo.
- Un año después comienza su “uso”.



Bitcoin

- Se necesita:
 - Dirección (identidad)
 - Cartera (software)
 - Negocios (comercio).



Bitcoin

- Se puede:
 - Comprar
 - Minar
- Limitada a 21 millones de bitcoins (en 2140).
- Actualmente hay ~11 millones.



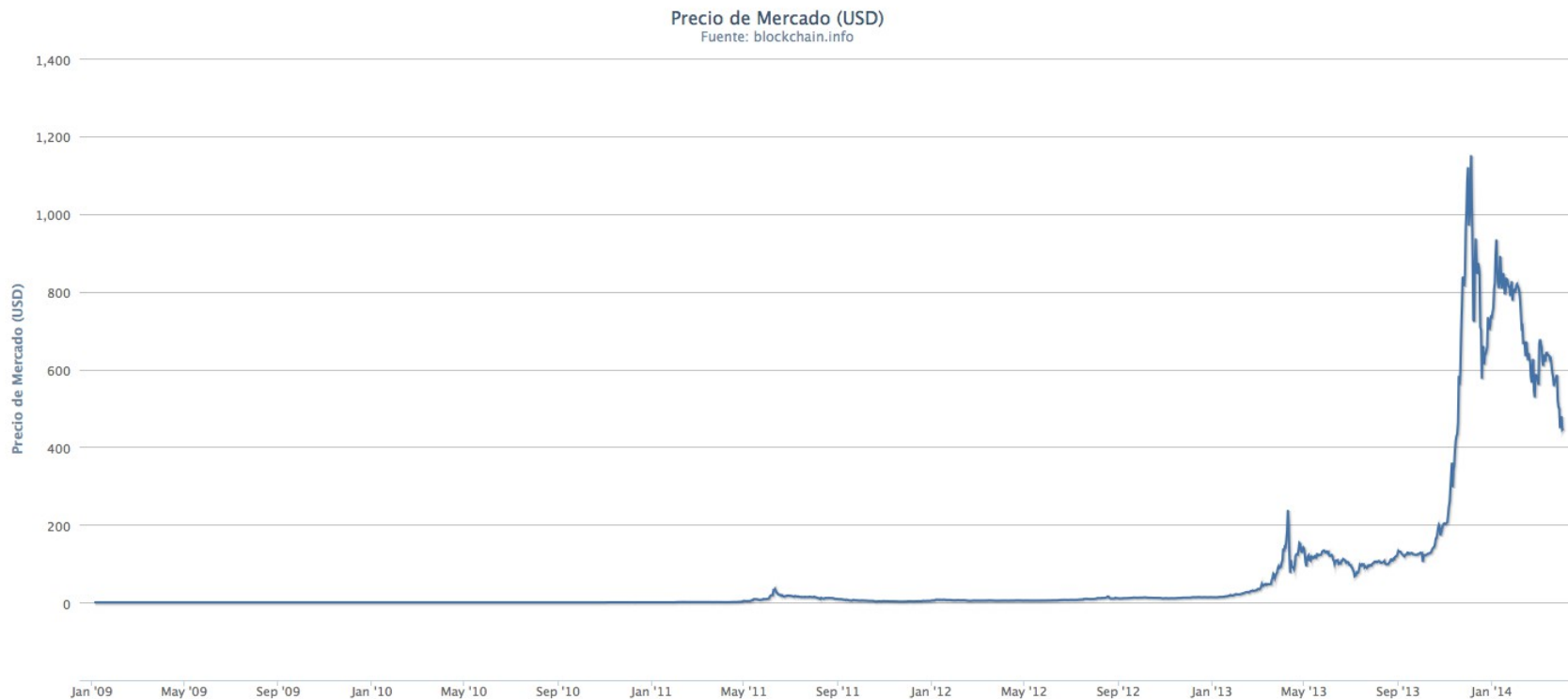
Bitcoin

- Auto-sustentable.
- Previene inflación.
- Cifrada.



Bitcoin

- Preev.com
(1/Abril/2014)
 - 1 BTC = 478.4 USD



Bitcoin

- Descentralizada = Sin infraestructura que pueda ser destruida.
- Anónima = Sin nombres, sólo un identificador de tu billetera.



Bitcoin

- Se puede:
 - Vender.
 - Transferir.
 - Intercambiar.
 - Hoteles.
 - Electrónicos.



Bitcoin

- ¿Legal?

- Es sólo un conjunto de bits.
- USA: ojo con el lavado del dinero.
- México: no reconocida; sin respaldo.

- ¿Legal?

- Rusia y China: prohibida.
- Algunos otros: impuestos.
- <http://bitcoinfacil.net/igualdad-bitcoin-mundo/>

Bitcoin

- En el Mundo:
 - 4.85 BTC para una semana en San Francisco.
 - Berlín, mayor concentración de comerciantes que aceptan Bitcoins.



Bitcoin

- En México:
 - Un cajero automático en Tijuana.



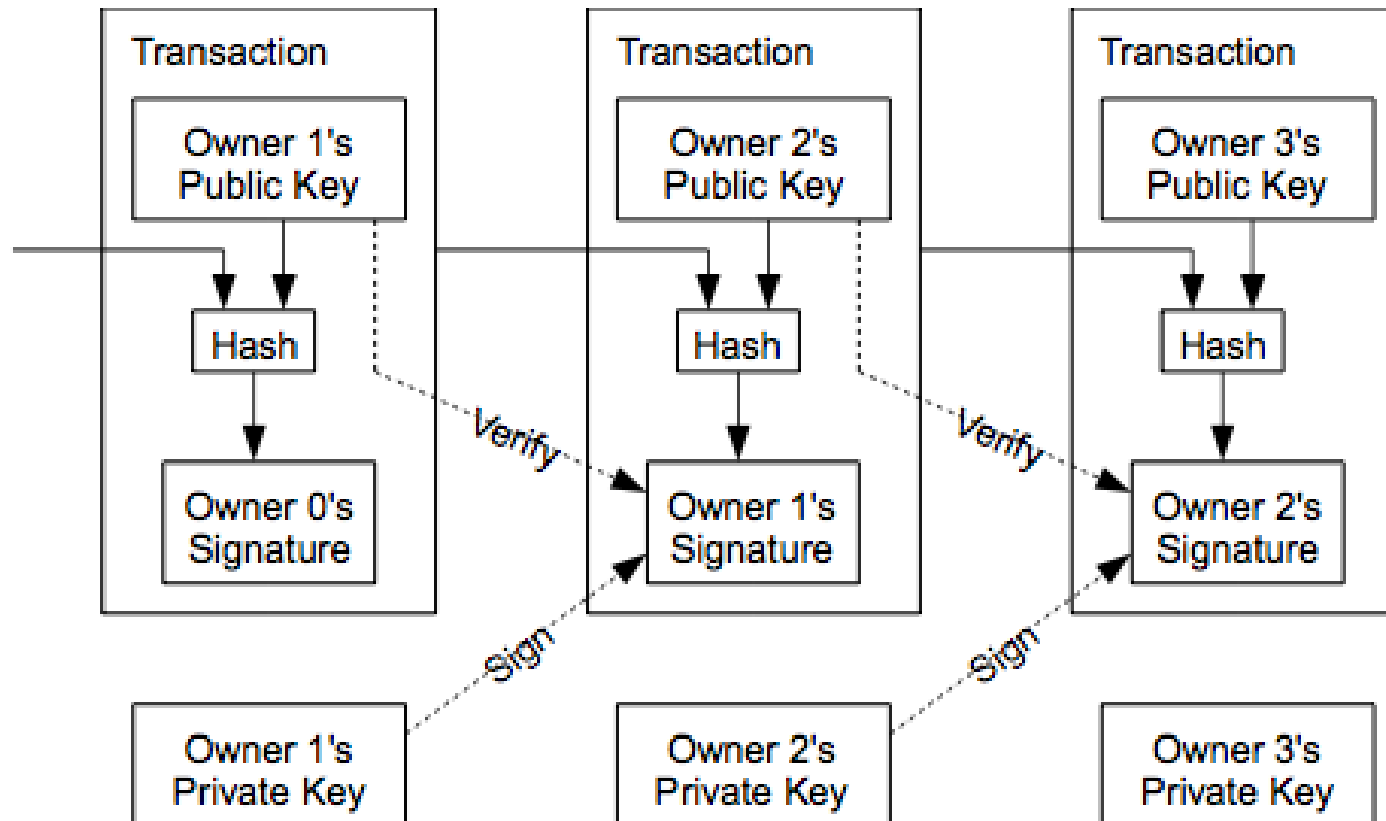
Bitcoin

- En Guadalajara:
 - Casa Victoria (comida).
 - El Hostelito (hospedaje).
 - Se pueden comprar en Oxxo (BitcoinPlus.mx).

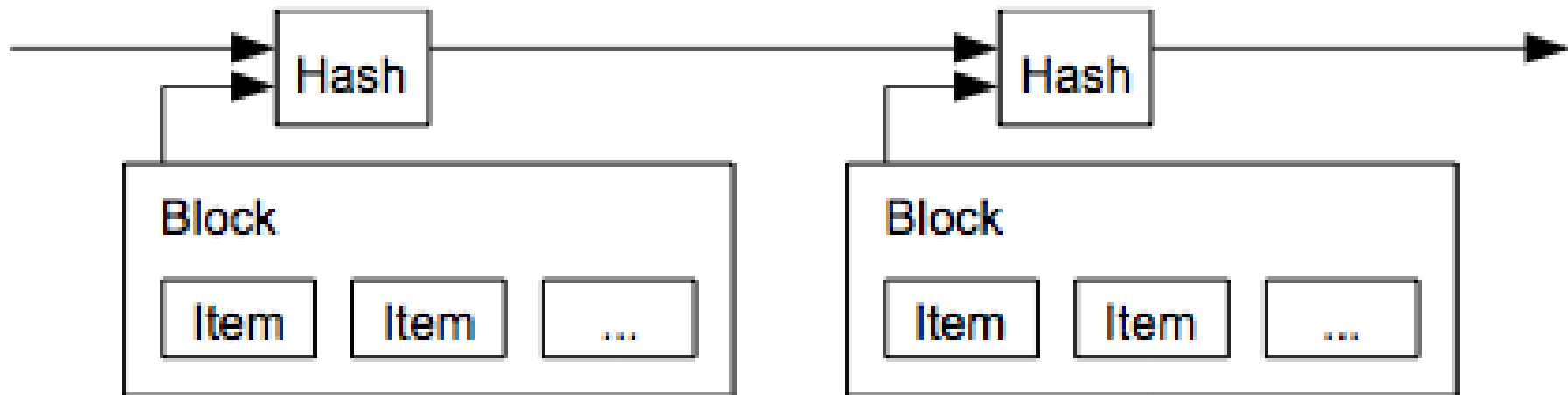


Técnicamente, ¿cómo funciona?

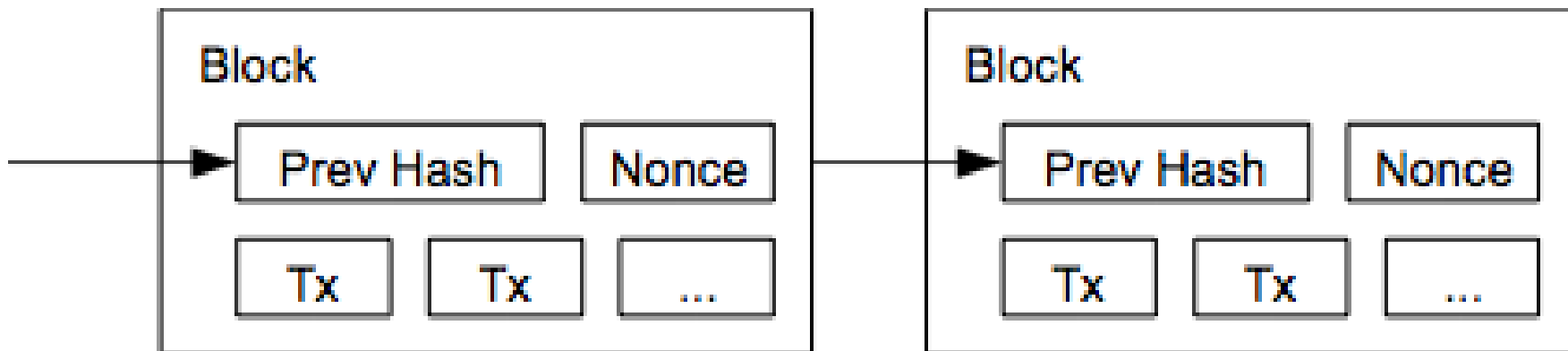
El esquema general



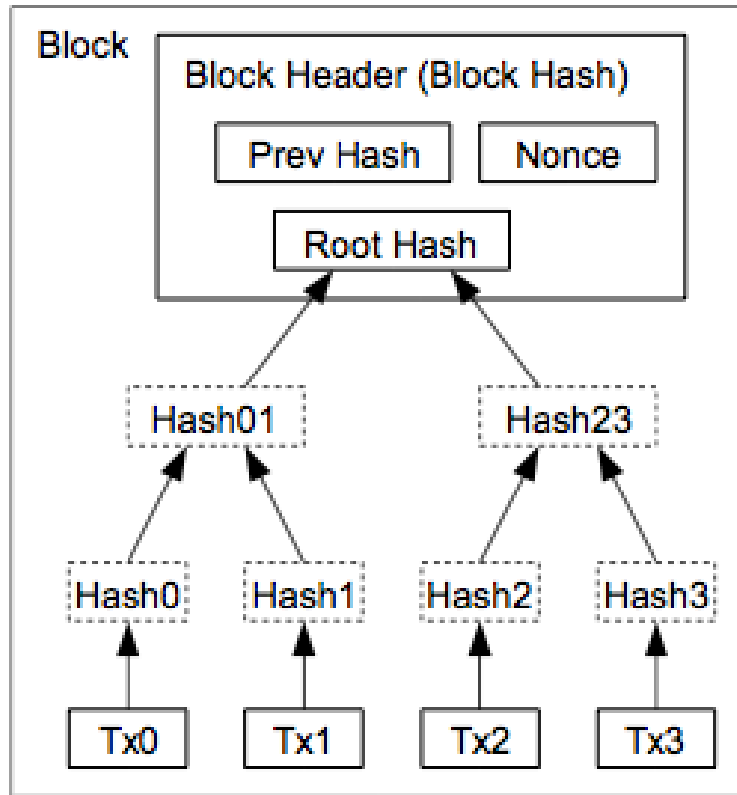
El esquema general



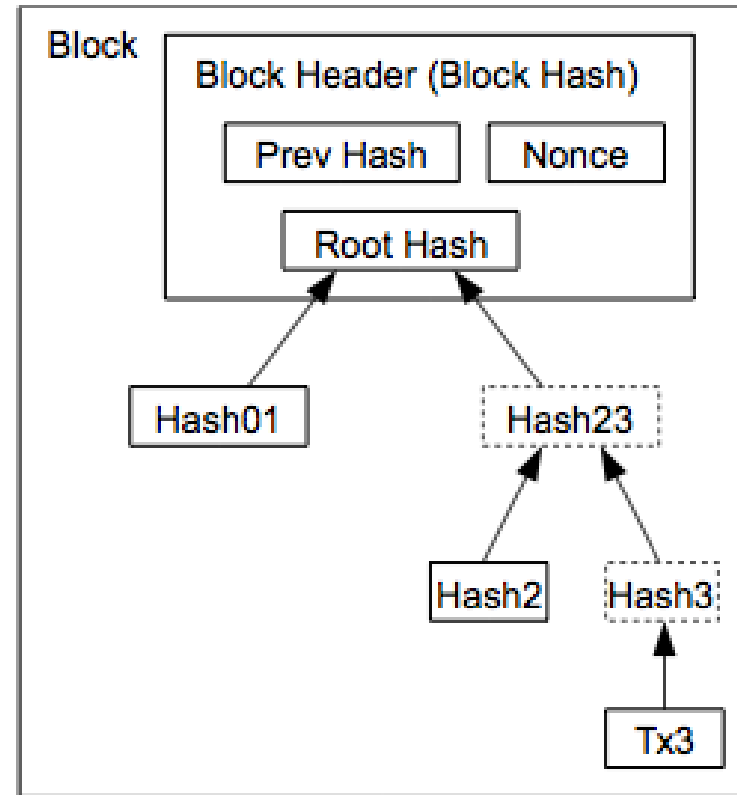
El esquema general



El esquema general



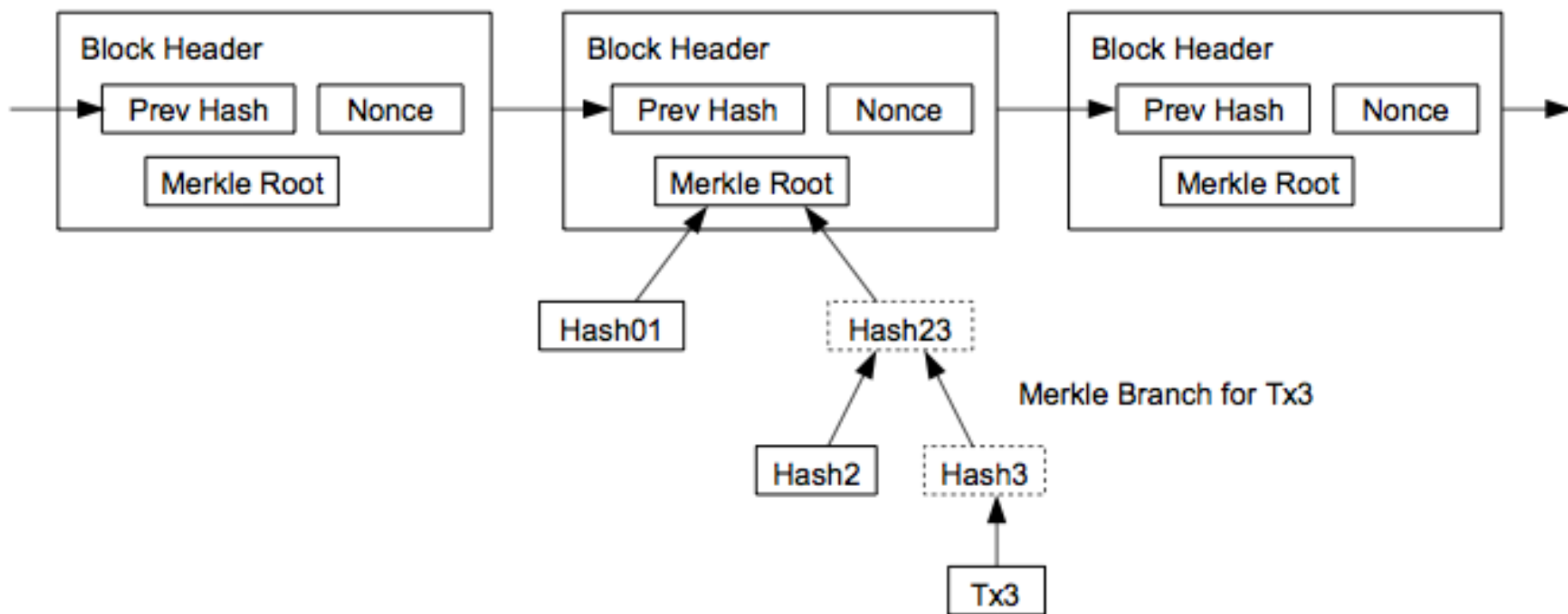
Transactions Hashed in a Merkle Tree



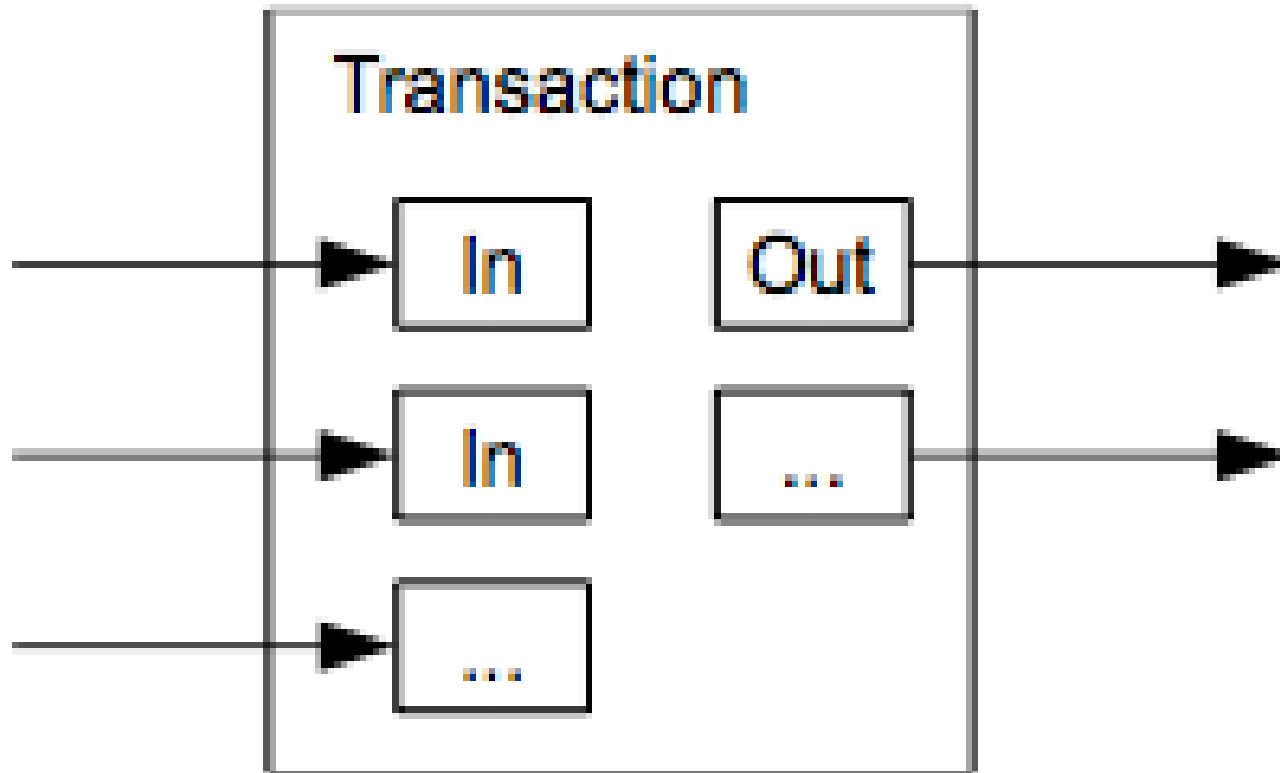
After Pruning Tx0-2 from the Block

El esquema general

Longest Proof-of-Work Chain



El esquema general



¿Qué es “minar”?

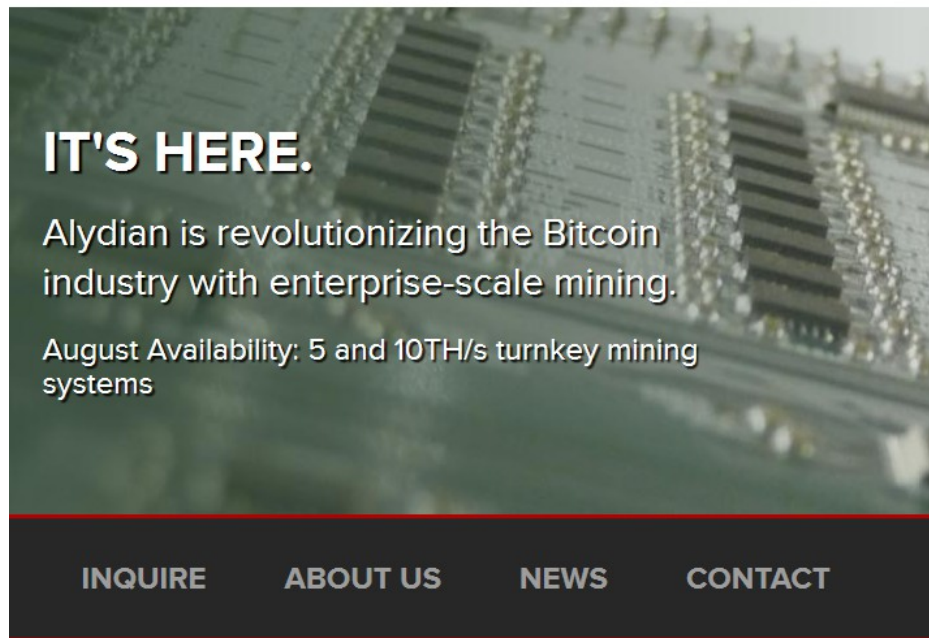
Minar



- Hash, hashing, red, más hashing, energía, más hashing, un poco más de energía, y un toque más de hashing con mucha energía.

Minar

alydian



IT'S HERE.

Alydian is revolutionizing the Bitcoin industry with enterprise-scale mining.

August Availability: 5 and 10TH/s turnkey mining systems

[INQUIRE](#) [ABOUT US](#) [NEWS](#) [CONTACT](#)

- Inicialmente CPU's.
- Le siguieron los GPU's.
- Tuvo mucho éxito los FPGA's.
- Lo de hoy son los ASIC's.
- Bitcoin vs energía.

¿Otras cripto-monedas?

Litecoin



- Bitcoin es el “oro”, Litecoin es la “plata”.
- scrypt vs sha256d.
- 84 millones.

Dogecoin



- 99,000 millones + 5,000 millones por año.
- Recompensas aleatorias.
- Diciembre 2013.

Otras cripto-divisas

- Namecoin
- PPCoin
- Mastercoin
- Hashcoin
- Coino
- RonPaulCoin
- Betacoin
- Nxt
- Globe
- Megacoin
- AnonCoin
- Y una largo etcétera.

Para saber más...

- <https://bitcoin.org>
- https://en.bitcoin.it/wiki/List_of_alternative_cryptocurrencies
- <http://bitcoinmexico.org/>

¡Gracias por su atención!

¿Preguntas?

Siguiente charla:

Seguridad informática para no-informáticos

(Cifrado; Firmado de correo y documentos; Manejo de contraseñas.)

Consultar la fecha en:

<http://www.csgdl.org/>