

Bitcoin, Energía y Argentina

Claudio Pastorino

Grupo de Teoría y Simulación en Materia Blanda
Departamento de Física de Materia Condensada
GiyA-GayANN, INN-CONICET-CNEA
CAC CNEA

Esteban Mocskos

Laboratorio Interdisciplinario de Cómputo de Alto
Desempeño,
Departamento de Computación, FCEyN-UBA.
Centro de Simulación Computacional p/aplic Tecnológicas,
CSC-CONICET

Advertencia: el contenido de estas diapositivas no representa recomendación alguna de compra o venta de ningún activo financiero.



Comisión Nacional
de Energía Atómica

CONICET



Criptomonedas

- Las criptomonedas son relevantes en varios contextos: económico, tecnológico y energético.
- **Las tecnologías de blockchain y criptografía** abren algo nuevo que hasta hace poco no podía hacerse: transferencia de valor a través de internet **sin intervención de terceros**.
- Existen muchas criptomonedas o tokens (~15k) con objetivos, grados de madurez y relevancia muy diferentes.
- **Bitcoin** es la primera (2009), madura, robusta, con la red de nodos más grande y la de mayor valor (market cap)

Impacto y disrupción en

Discusiones:

- Geopolítica
- Economía
- Tecnología
- Ética
- Energía
- Medio Ambiente

- Muy válidas
- No están saldadas
- No las trataremos en su mayoría

Para abordar el tema, reducimos a:



- Bitcoin
- Energía
- Argentina

Bitcoin: oro digital (?)

- Bitcoin tiene las propiedades que hicieron del oro una **reserva de valor** histórica:
 - Escaso
 - Fungible
 - Durable
 - Divisible (1 satoshi = 1/100.000.000 BTC, 1USD ~ 3000sats)
 - Transferible (digitalmente, trust-less)
 - Auto-custodiable
- **Innovación:** Primer objeto digital escaso
- **Combinación de:** criptografía, blockchain, sistemas distribuidos, matemática, computación de alto desempeño.

El Oro como reserva de valor

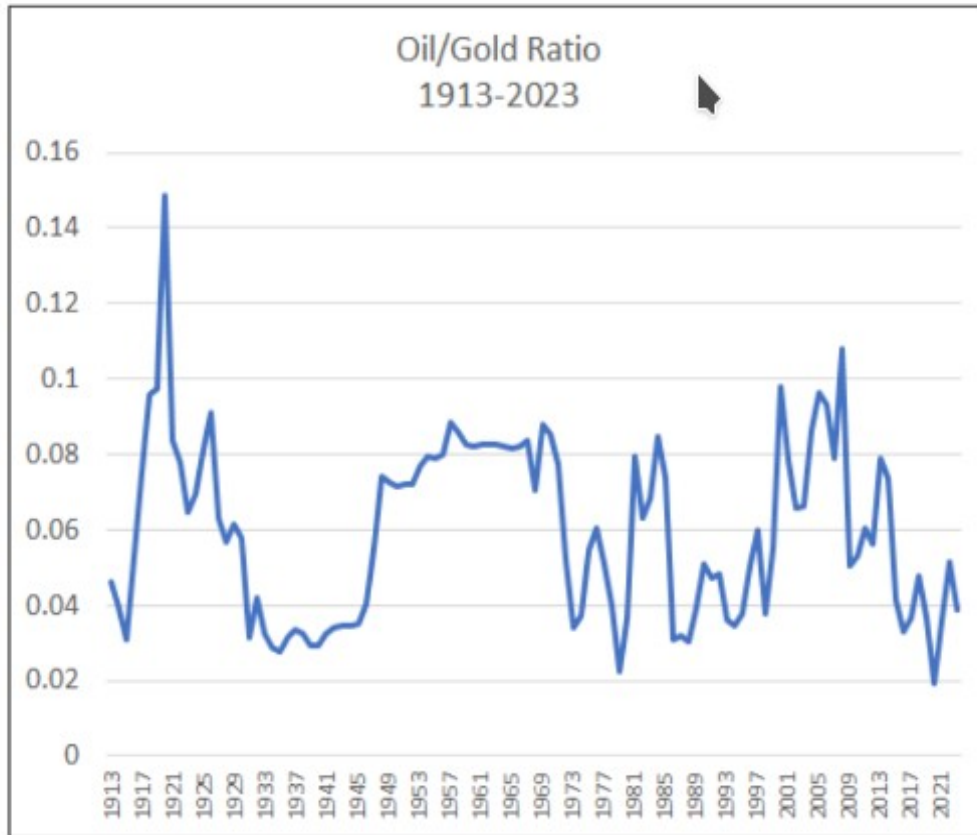
Metal escaso, durable (no se contamina, no se oxida)



Fuente: visualcapitalist.com

El Oro como reserva de valor

Precio del petróleo en oro



Precio del petróleo en dólares



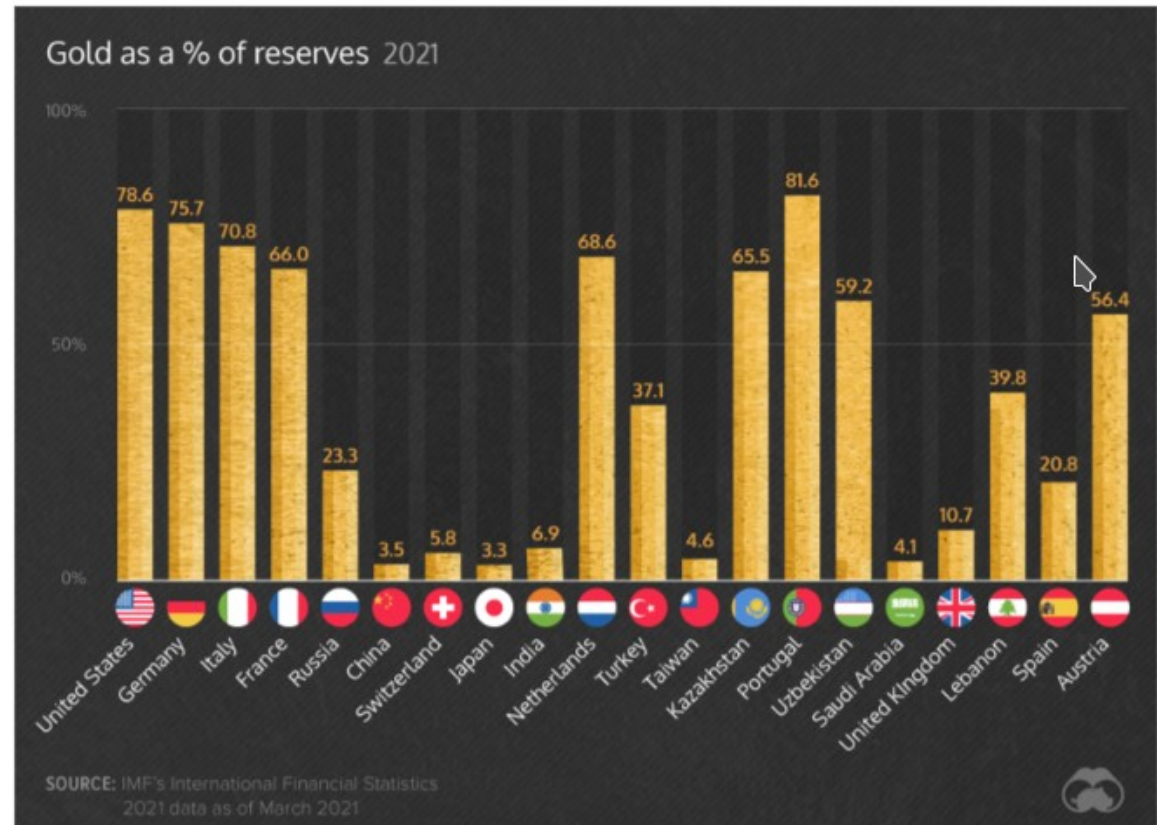
Fuente: Lyn Alden.

<https://www.lynalden.com/inflation-vs-interest-rates/>

El Oro como reserva de valor

Reservas de oro en bancos centrales (2021)

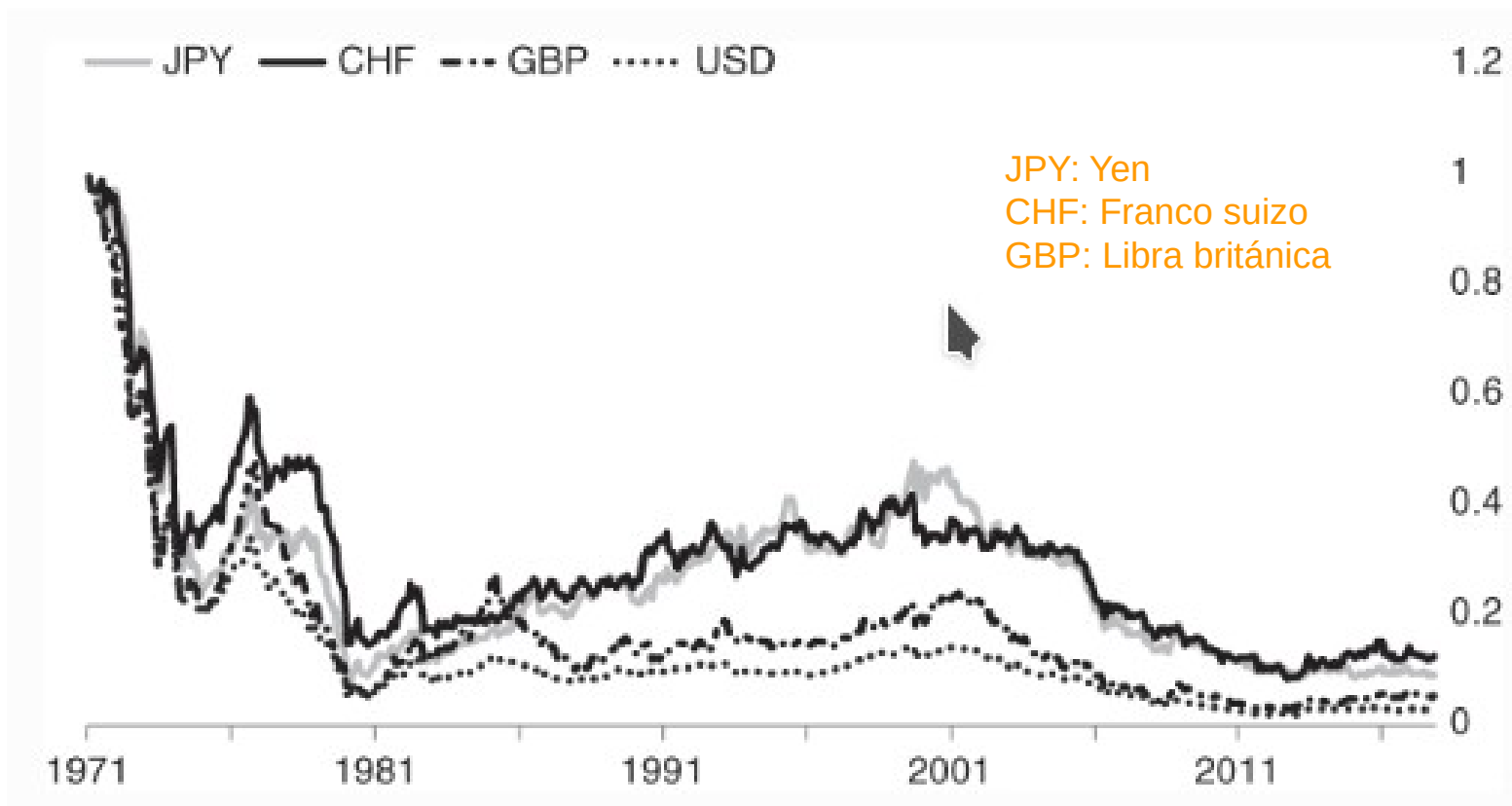
- **Naciones Europeas:** Mayoría con más del 50% de sus reservas en oro
- **China:** +393% desde el 2000
- **Rusia:** +443% desde el 2000
- **Argentina:** 61.74 tns (~Netherlands/10, 3806M USD, ~13% reservas)
- **Brasil:** 130 tns (~2.2% reservas)
- **USA:** 8133 tns



Fuente: [elements](#), [visualcapitalist](#), FMI

El Oro como reserva de valor

- Monedas más importantes medidas en oro
- 1971: USA abandona el patrón oro



Fuente: S. Ammous, The Bitcoin Standard, Wiley (2018)

La irrupción de Bitcoin: precio

BTC/XAU: Precio de bitcoin medido en oro



Fuente: [investing.com](https://www.investing.com)

La irrupción de Bitcoin: precio

BTC vs. tiempo

- Crecimiento ~ exponencial
- Volatilidad muy alta

Días rentables
Días no rentables

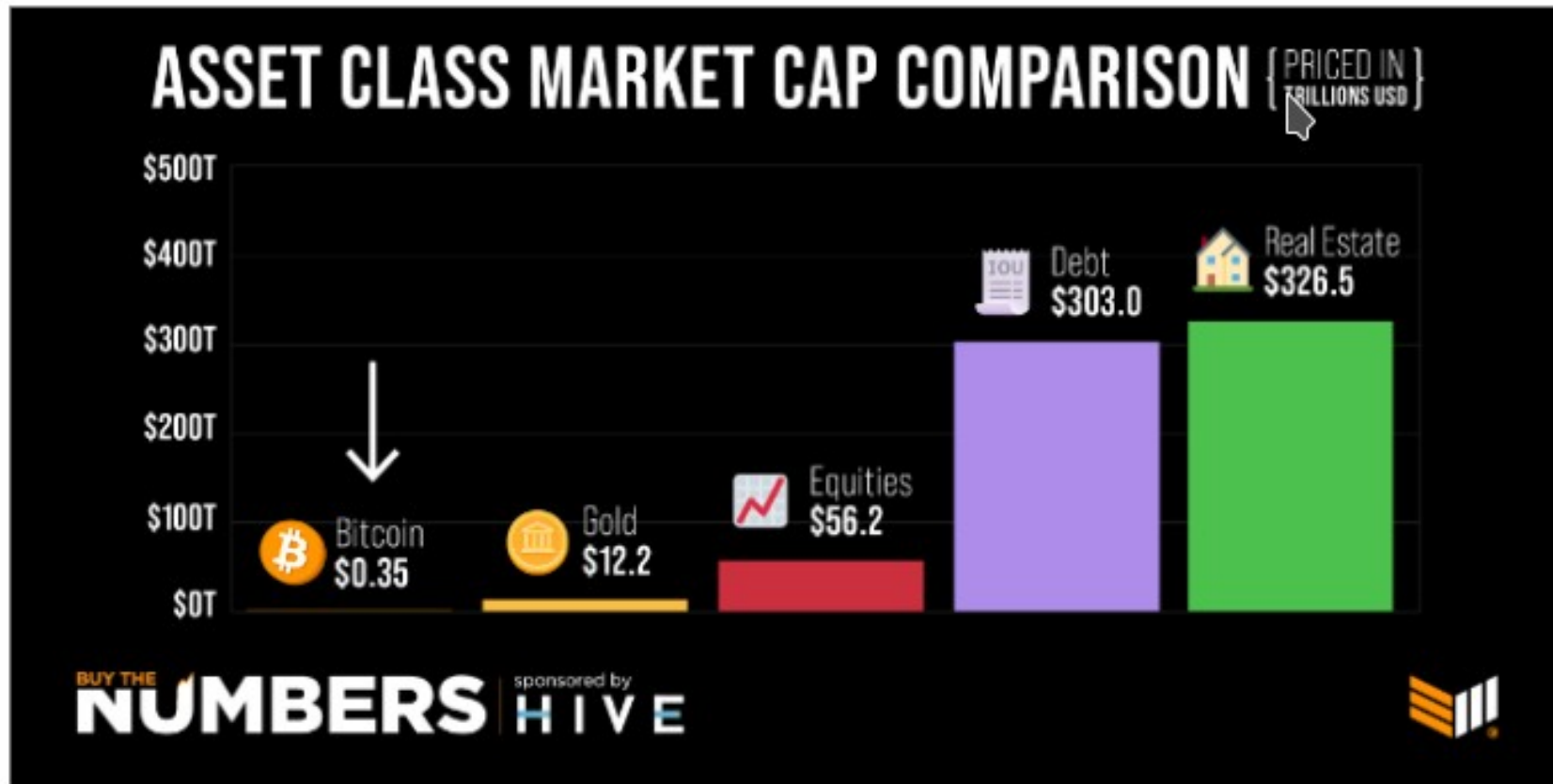


Fuente: lookintobitcoin.com

La irrupción de Bitcoin: su tamaño en la economía

1 BTC ~ 30000USD
market cap ~ 560B (Julio 25, 2023)
market cap ~ gold/20

Dato:
17/10/22

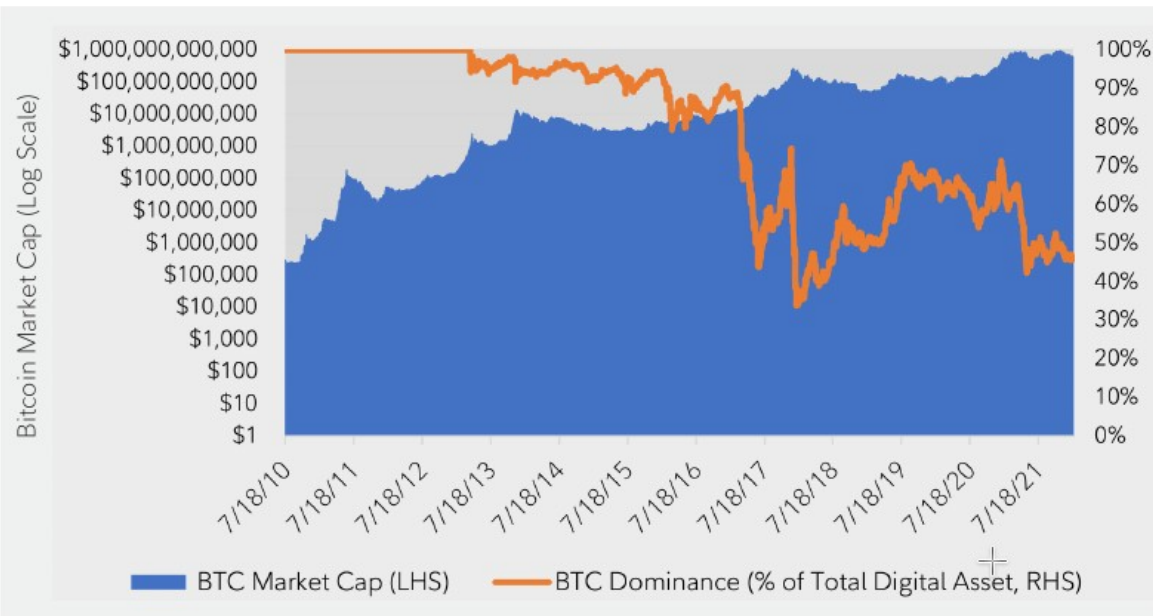


Fuente: bitcoinmagazine.com

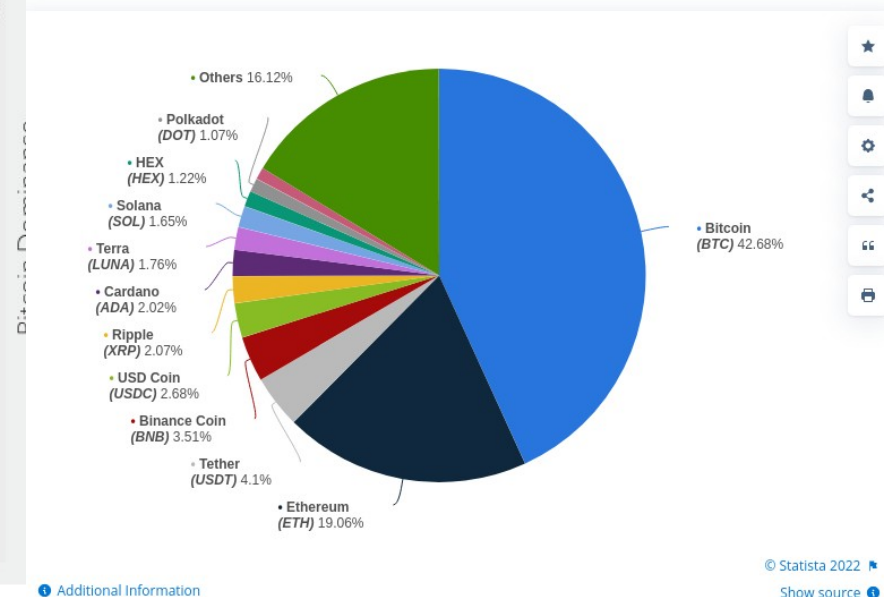
Bitcoin vs. otras criptos (altcoins)

- **Bitcoin dominance:** representa entre el 40 y 60% de la capitalización de mercado de todo el espacio de criptomonedas
- **Altcoins:** algunas presentan propuestas tecnológicas interesantes, son más homologables a empresas que a un commodity.
- **Ethereum:** Turing complete.
- **Stablecoins:** colateralizadas con un activo real. Ejemplo: dólar (USDT, USDC, DAI), oro (PAXG)
- Terreno de discusión: las altcoins tienen redes mucho más pequeñas.
Descentralización cuestionable.

BITCOIN DOMINANCE



Data Source: Coin Metrics, Date: 1/18/2022



Additional Information

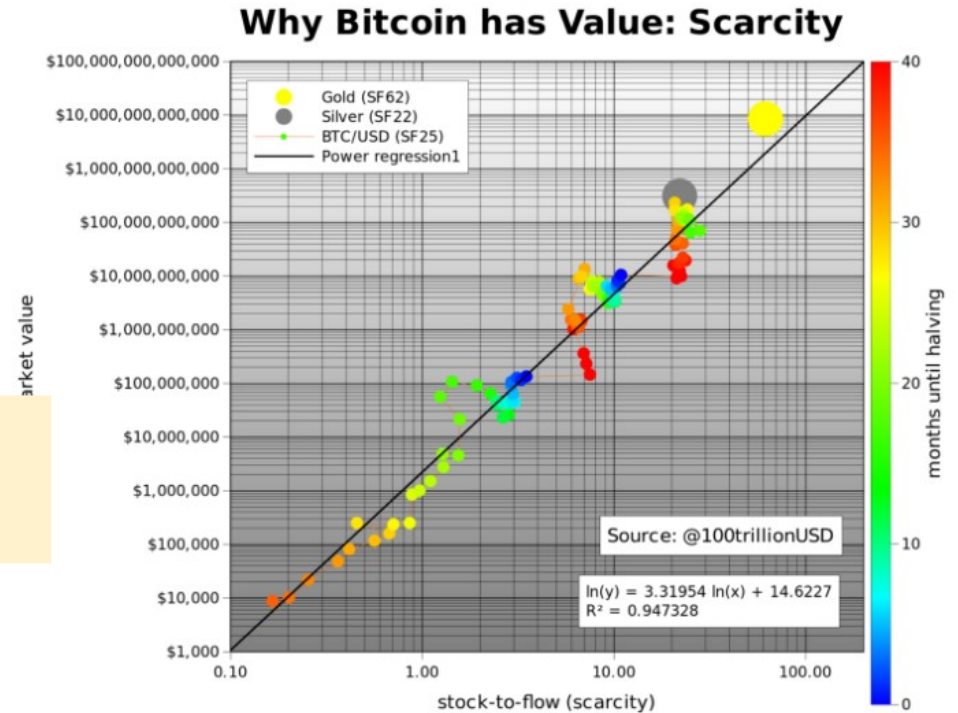
© Statista 2022
Show source

Modelo stock-to-flow

- Muy usado en commodities y metales.
- Vincula escasez con precios

$$SF = \frac{\text{stock}}{\text{flow}}$$

- Stock: tamaño de las reservas existentes.
- Flow: Producción anual (minado) del metal.













	Stock (tn)	Flow (tn)	SF	supply growth	Price \$/Oz	Market Value
gold	185,000	3,000	62	1.6%	\$ 1300	\$ 8,417,500,000,000
silver	550,000	25,000	22	4.5%	\$ 16	\$ 308,000,000,000
palladium	244	215	1.1	88.1%	\$ 1400	\$ 11,956,000,000
platinum	86	229	0.4	266.7%	\$ 800	\$ 2,400,000,000

Bitcoin: SF=56.1 (2/8/2023)

~ Abril 2024: SF=120
(luego del próximo halving)

Bitcoin y otras monedas

Propiedades de las monedas

	 GOLD	 BITCOIN	 FIAT CURRENCY	
 DURABLE	+	+	-	While all are physically durable, fiat currency over history has not maintained purchasing power durability
 DIVISIBLE	-	+	+	Physical gold is only divisible to small pieces; bitcoin is divisible to eight decimals
 FUNGIBLE	+	+	-	Gold and bitcoin are fungible, but fiat currency is not fungible with other fiat (US Dollar is not fungible with Canadian dollar)
 PORTABLE	-	+	+	Gold has a high value to weight ratio, but compared to the others is still heavy and cumbersome to transport
 VERIFIABLE	-	+	-	Both gold and fiat currency have been counterfeited; gold can be verified but only through cumbersome assay
 SCARCE	+	+	-	Gold is scarce, bitcoin is scarce and finite; the only constraint on fiat currency is willingness of government or central bank
 TRACK RECORD	+	-	-	Gold has the longest track record as money and maintaining purchasing power; bitcoin's history is the shortest; fiat currency has a poor track record ²

Características principales de Bitcoin

- 21 millones: la cantidad **máxima** de bitcoins.
- Sin censura: nadie puede **censurar** transacciones válidas.
- Código abierto: el código fuente de Bitcoin siempre debe ser **accesible** para todos.
- Sin permiso: nadie puede **impedir** la participación en la red.
- Pseudoanónimo: no se requiere **identificación** para participar en la red Bitcoin.
- Pagos **irreversibles**: las transacciones confirmadas no pueden ser modificadas ni eliminadas. La historia es **imborrable**.

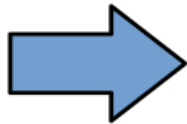
¿Qué es una transacción?

Trato por el que dos partes, llegan a un **acuerdo comercial**

Banco

Cuenta A

10 \$
-10 \$



Cuenta B

0 \$
10 \$

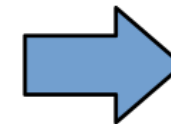
Saldo: 0 \$

Saldo: 10 \$

Bitcoin

A

10 \$



B

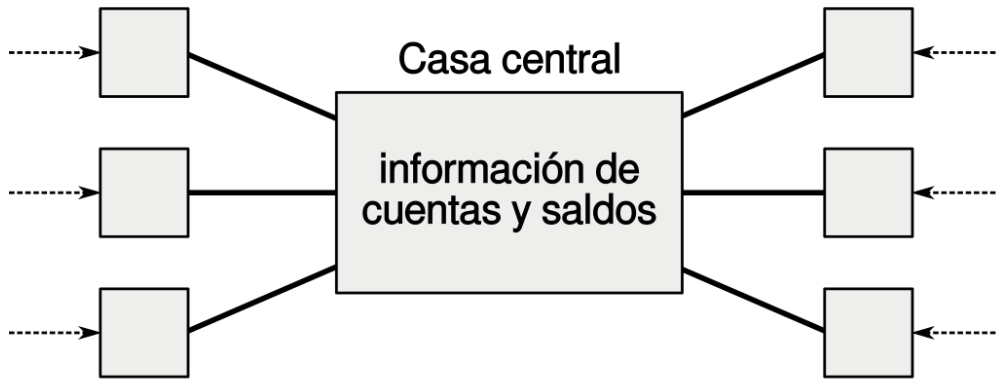
10 \$
para B
firma A

Saldo: 0 \$

Saldo: 10 \$

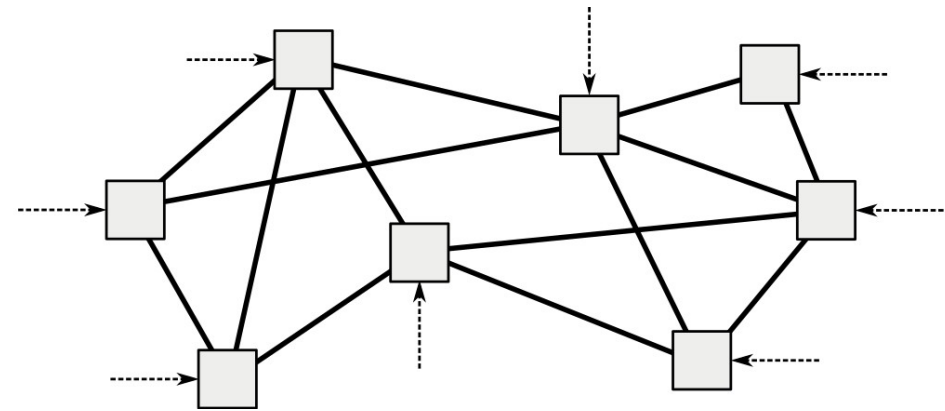
Red bancaria tradicional vs Bitcoin

Banco



En un banco la información está **centralizada** en la casa central

Bitcoin



En Bitcoin cada nodo tiene **toda** la información sobre cuentas y saldos

¿Qué es una función de *Hash*?

Una función de HASH toma una secuencia de valores y genera un número de **tamaño fijo**.

Ejemplos:

- HASH(0000 0000 0000 0000 0000 0000) -> 2413
- HASH(0000 0000 0000 0000 0000 0001) -> 9402
- HASH(0000 0000 0000 0000 0000 0002) ->1465

- Es fácil de calcular
- No se puede predecir el resultado
- Un cambio mínimo en la entrada, produce un cambio drástico en la salida

¿Ejemplos de *Hash*?

Hay varias implementaciones **directamente disponibles** de funciones hash, en general, se mira el **tamaño** del hash generado.

Con un archivo con el siguiente contenido (como texto):

```
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

Calculo el md5sum -> 6218f03f61297331107794c7dec4cd8c

Con un archivo con el siguiente contenido (como texto):

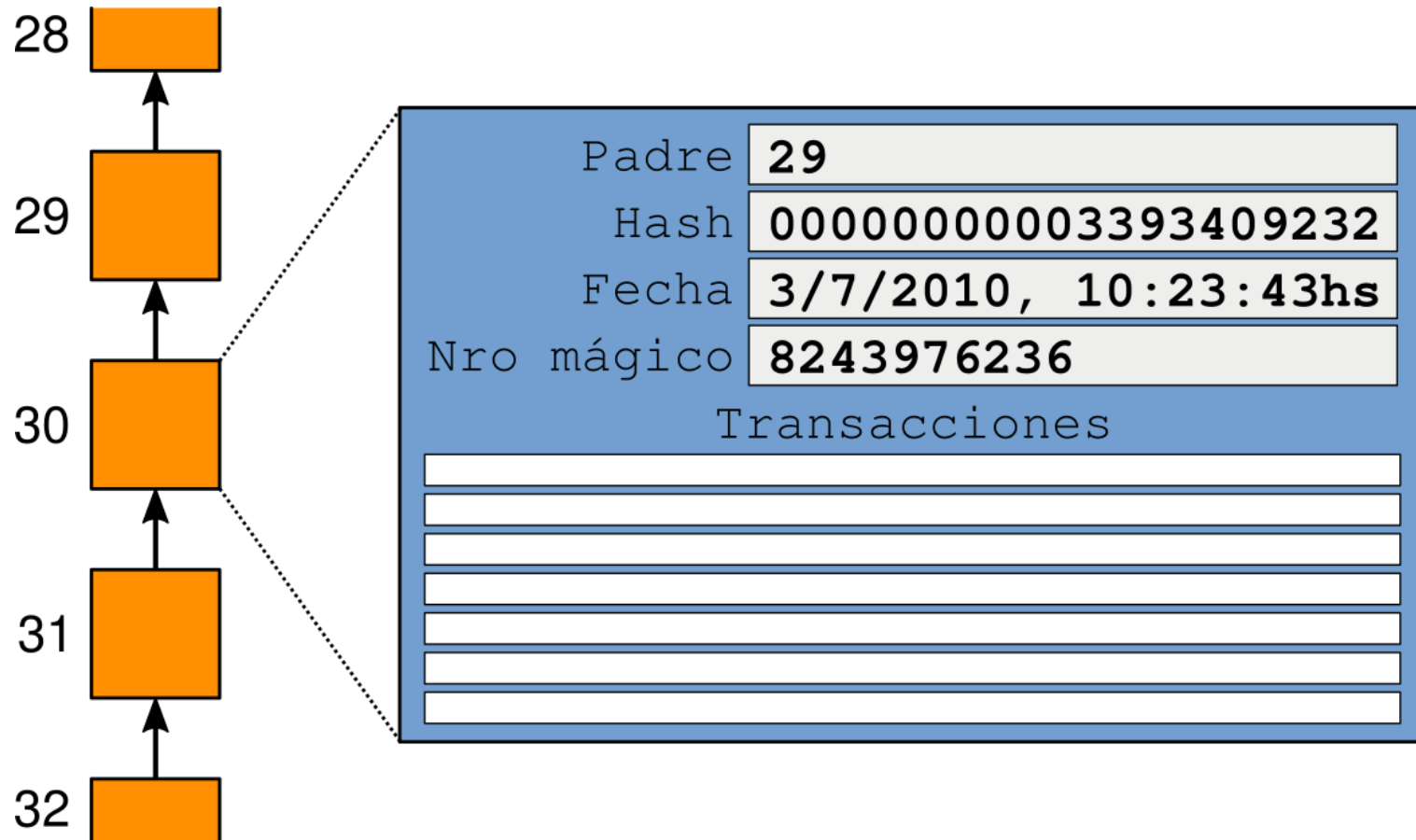
```
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000  
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

Calculo el md5sum -> 664964f3959ff7208ea59400e74d5d0f

Le cambio un solo digito al principio.

Calculo el md5sum -> 67ba719ec57c53af3c7c517a42559c65

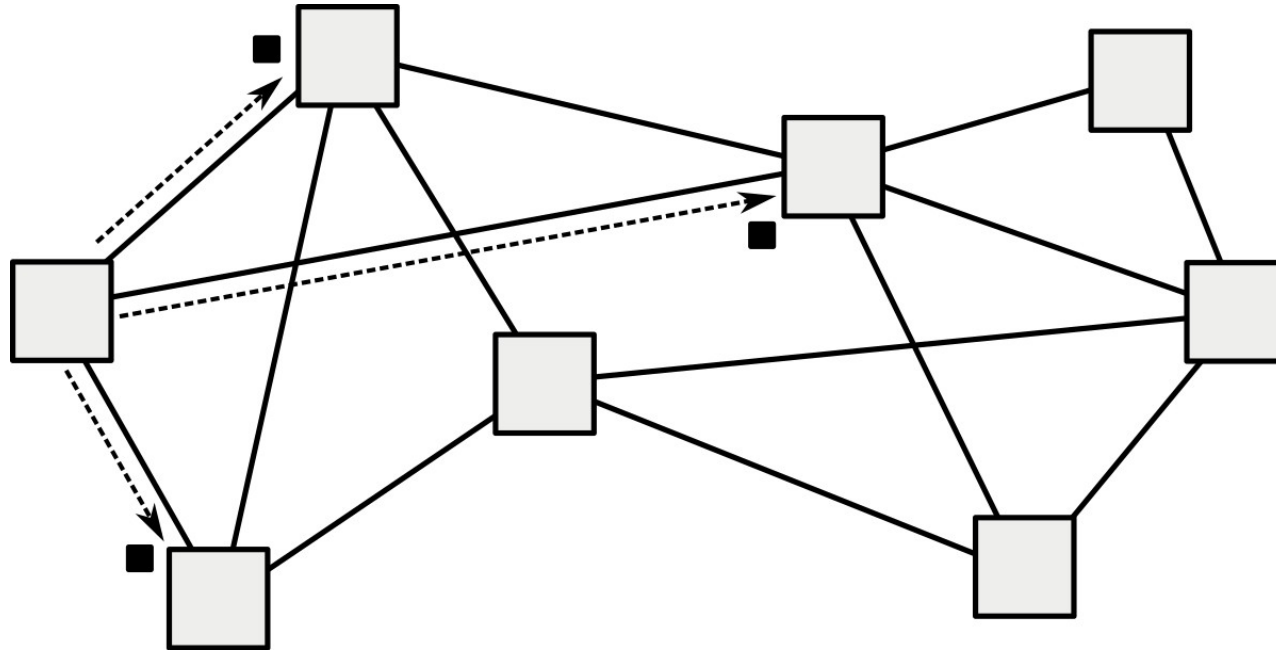
¿Dónde se guardan las transacciones?



- Las transacciones se guardan en **bloques**.
- Cada bloque se **relaciona** con el anterior.

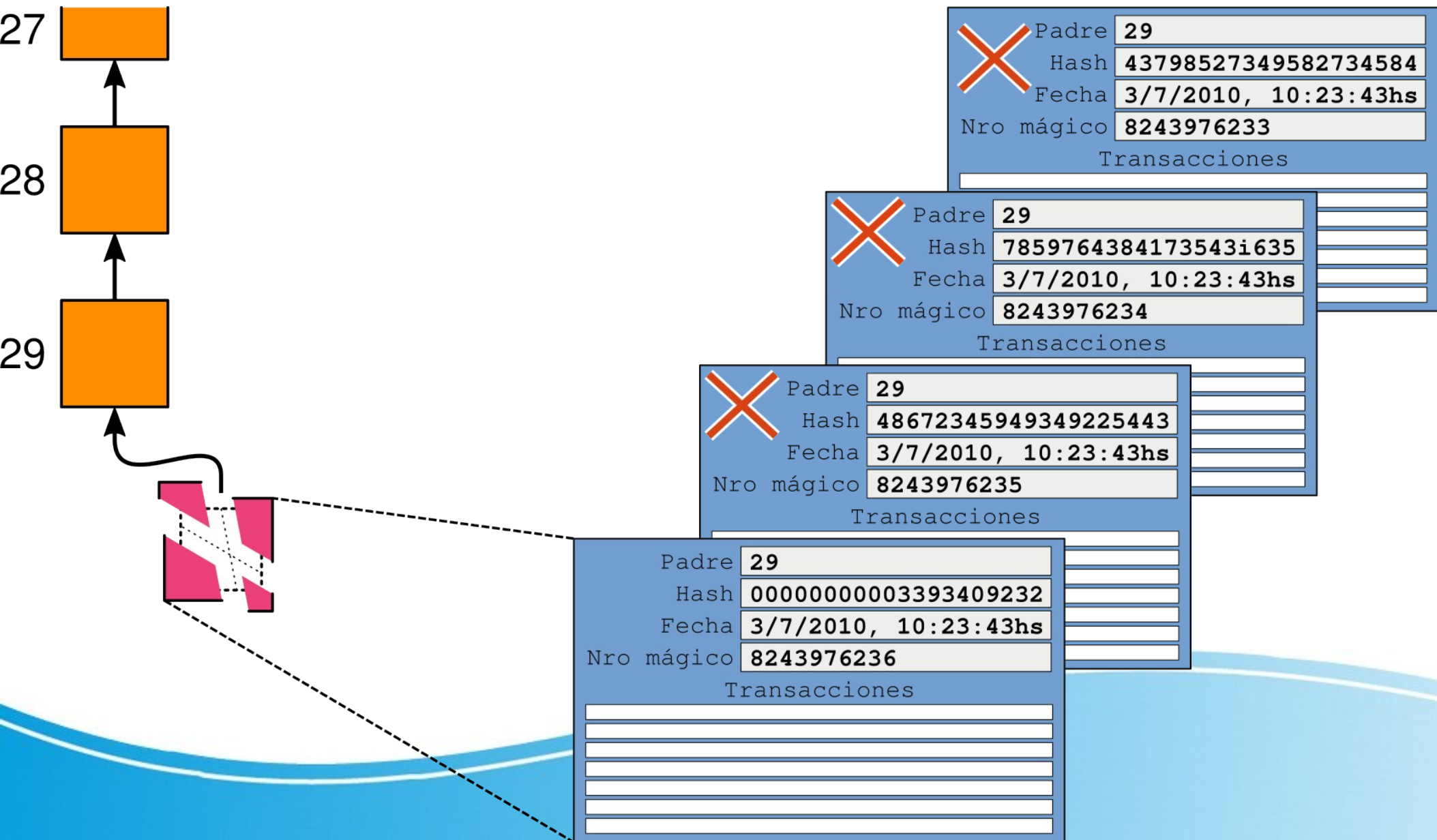
¿Cómo se crean bitcoins? Minado

- Algunos nodos (mineros) de la red **crean** bloques nuevos
- Los nuevos bloques **aparecen** cada 10 minutos (aprox)

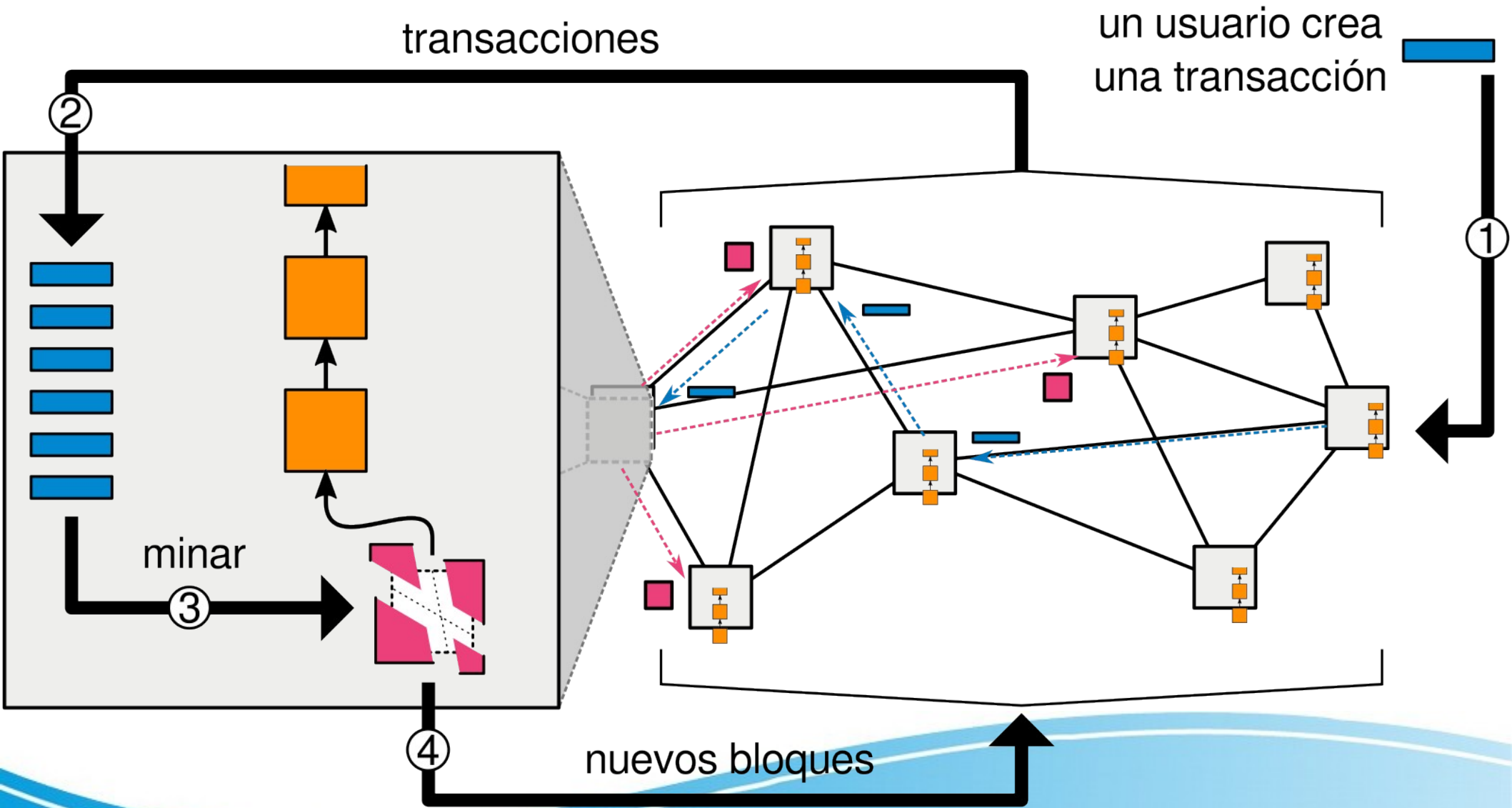


Cuando un minero *mina* un bloque, le avisa a toda la red que lo encontró.

Blockchain: proceso de minado

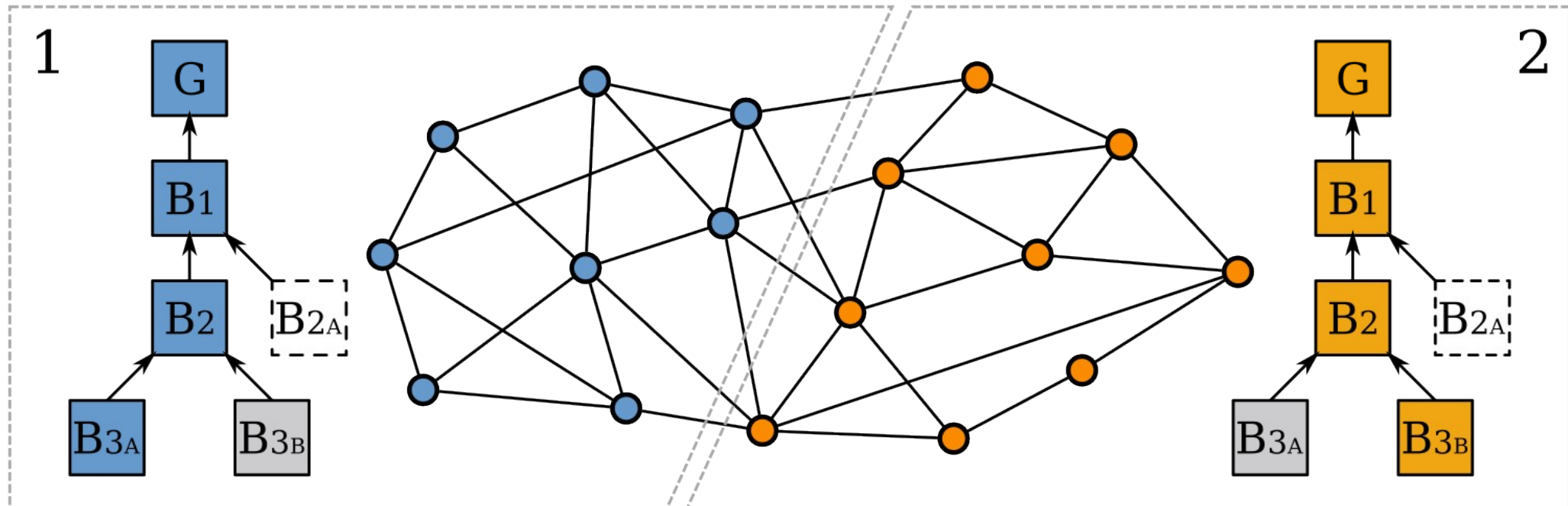


Todo el proceso junto



¿Qué pasa si dos mineros ganan?

Fork



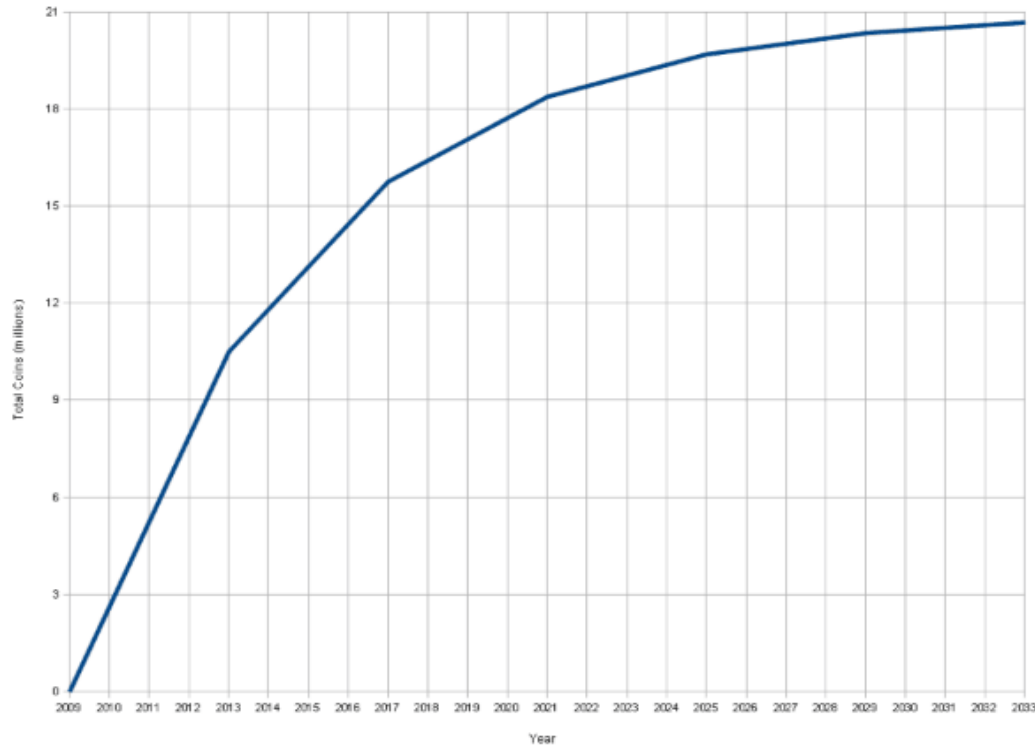
Cada **fork** considera distintas cadenas principales como **válidas**. alguna de las cadenas tendrá una dificultad mayor y es la que se elige como **principal**.

Bitcoin: detalles

- Tasa de inflación de bitcoin: 1.8% anual y bajando.
- La producción de bitcoin está limitada a **21 millones**.
- **Descentralización**. Codificado en la red. Open source.
- **Blockchain**: libro de registros digital (ledger), inmodificable, distribuido, no hackeable.
- **Consenso**. Los participantes de la red pueden cambiar por consenso (**total**) alguna regla. Todo el sistema se debe poner de acuerdo, sino **hard fork**
- **Resistente a censura**. Ni personas, ni corporaciones ni gobiernos son dueños o controlan la red bitcoin.
- **Network effect**. A partir de cierto tamaño, el valor de una red crece exponencialmente con el número de usuarios. En redes monetarias es aún mayor el incentivo de elegir la divisa correcta. Si la red bitcoin crece lo suficiente, disminuye la probabilidad de que otra la reemplace.

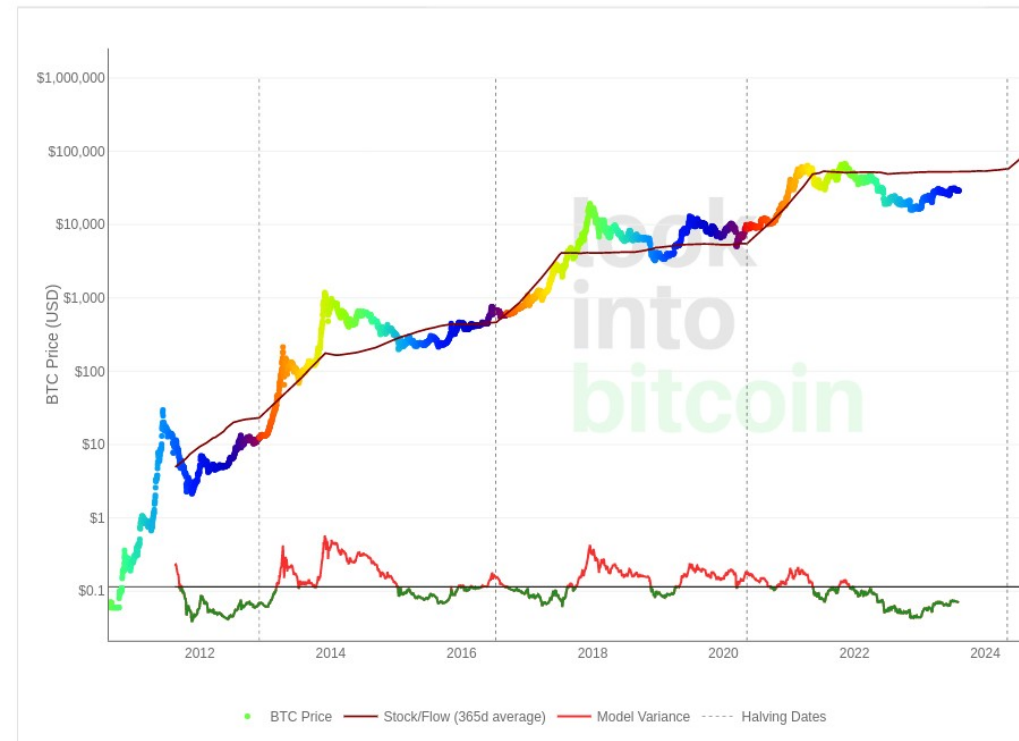
Bitcoin emitidos vs tiempo

- Se generaron más de 19.4M (8/2023)
- Mas del 92% del total posible (21M).



Stock-to-Flow Model

Source: lookintobitcoin.com



Fuente: lookintobitcoin.com

Bitcoin y energía

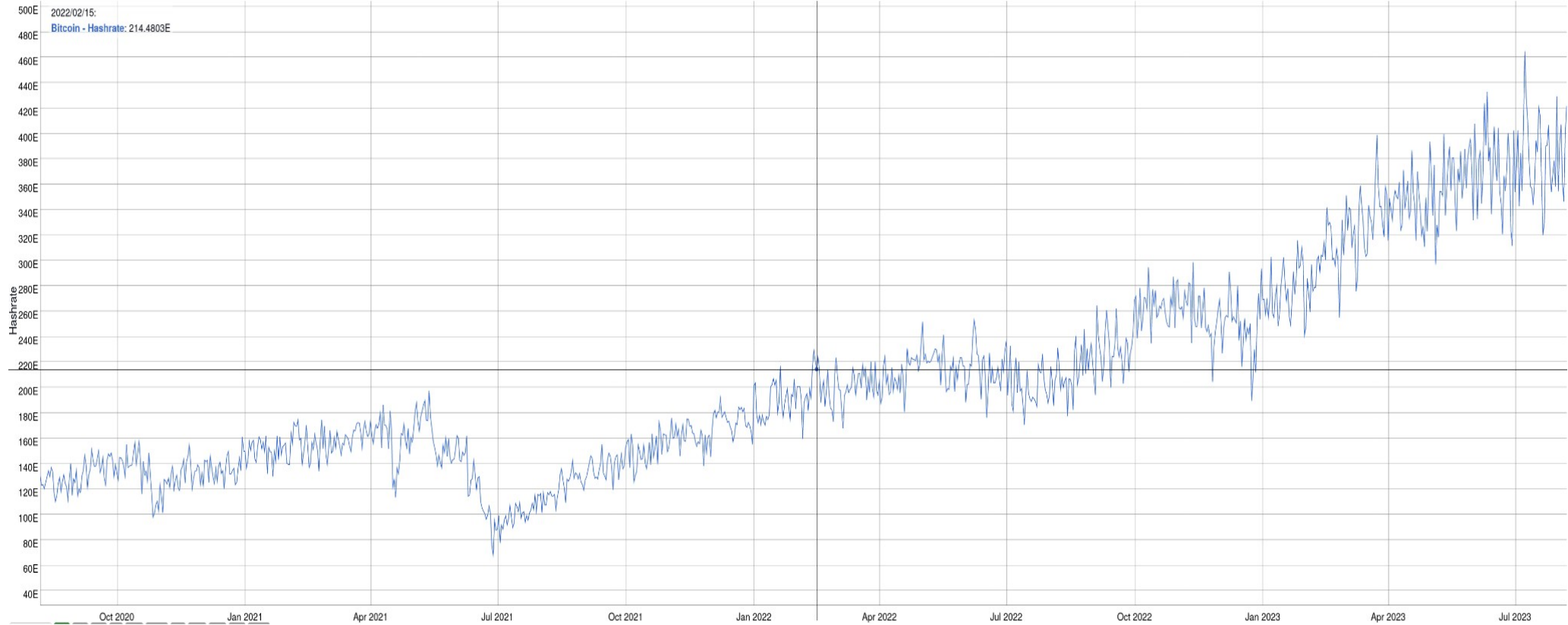
- Bitcoin network crea un nuevo bloque cada 10min (en promedio) y lo agrega a la **blockchain** (cientos de miles de bloques desde 2009).
- **Los mineros** (nodos especializados) producen un nuevo bloque resolviendo un problema criptográfico. Empaquetan también transacciones en ese bloque (y validan las transacciones).
- **Ajuste de dificultad:** Si muchos mineros salen (o entran) de (a) la red, la red regula el problema criptográfico.
- **Proof-of-work:** los nodos de la red hacen cómputo (usan electricidad) para resolver el problema criptográfico. Parece un desaprovechamiento de energía, pero garantiza seguridad y descentralización (El trabajo es árbitro de la veracidad). No hay autoridad central que decide la validez de un bloque.
- **Proof-of-Stake:** las crypto verdes actuales, cambian el esquema de validación.

Recursos en Bitcoin

Bitcoin Hashrate historical chart

Average hashrate (hash/s) per day | 388.645 Ehash/s -6.92% in 24 hours

Share: [Twitter](#) [Reddit](#) [VK](#) [Facebook](#) [LinkedIn](#)



Respuesta de Bitcoin - Dificultad



Bitcoin y energía (por qué usa?)

- La cadena más larga, es la que contiene más trabajo y la que cumple el criterio de consenso de la red
- A mayor energía consumida, más segura es la red bitcoin respecto de los ataques.
- Atacar con posibilidades bitcoin, requiere el 51% del poder de procesamiento de la red.
- **Oro:** Como histórica reserva de valor, también puede pensarse como parametrización de energía. Cuesta mucho obtenerlo y es contaminante.

Bitcoin y Energía

- Necesita energía para sostener la descentralización y seguridad.
- Bitcoin: consume **casi tanta energía** como Argentina (La energía de países bajos)
- La puede utilizar de una forma **muy versátil** en comparación con otros consumidores de energía.
- Los mineros pueden **acercarse** a las fuentes de energía varada

Ganancias por Minado

Bitcoin Mining Profitability historical chart

Mining Profitability | 0.0658 USD/Day for 1 THash/s

Share: [Twitter](#) [Reddit](#) [VK](#) [Facebook](#) [LinkedIn](#)



Comisiones



Bitcoin y Energía

- Minar requiere sólo una conexión “básica” de internet, una vez que se sincroniza la Blockchain, **no usa tanto ancho de banda.**
- Algunas de las fuentes de **energía más baratas** están fuera de la red eléctrica.
- Bitcoin permite
 - Aprovechar **energía varada** (stranded energy)
 - Hacer viables **nuevas fuentes de energía** desconectadas de la red
 - Optimizar diseño y uso de fuentes de **energía integradas** a la red

Ejemplos: quema de gas en pozos petroleros(1/4)

- Muchos depósitos de petróleo tienen gas.
- Si hay cantidades grandes, tiene sentido hacer un gasoducto. Si no, se ventea o se quema.
- Efecto invernadero:
 $\text{CH}_4 \sim 28x \text{CO}_2$ (en 100 años).
- Dato: 1480M piés cúbicos de gas natural fueron venteados o quemados en USA (2019)
- $\sim 150\text{TWh}$ de energía por año
- Cambridge estimó que el potencial de recuperación de gas varado es **8x** el consumo de la red Bitcoin.
- Ya hay empresas que se acoplan con las productoras de gas. [Exxon](#), [Gigaenergy](#)



Production flaring at a crude oil extraction sites offshore from Vietnam in the South China Sea. (wikipedia)

We bring the **B** market to the molecule

Great American Mining monetizes wasted, stranded and undervalued gas throughout the oil and gas industry by using it as a power generation source for bitcoin mining. We bring the market and our expertise to the molecule. Our solutions make producers more efficient and profitable while helping to reduce flaring and venting throughout the oil and gas value chain.

[Learn about our mission](#)

GREAT AMERICAN MINING

Ejemplos: energía hidroeléctrica en China

- Energía hidroeléctrica varada en china (provincia de Sichuan).
- En temporada de lluvias producían mucha más energía de la que podían utilizar.
- Mineros de bitcoin se movían hacia allí para minar con energía barata.

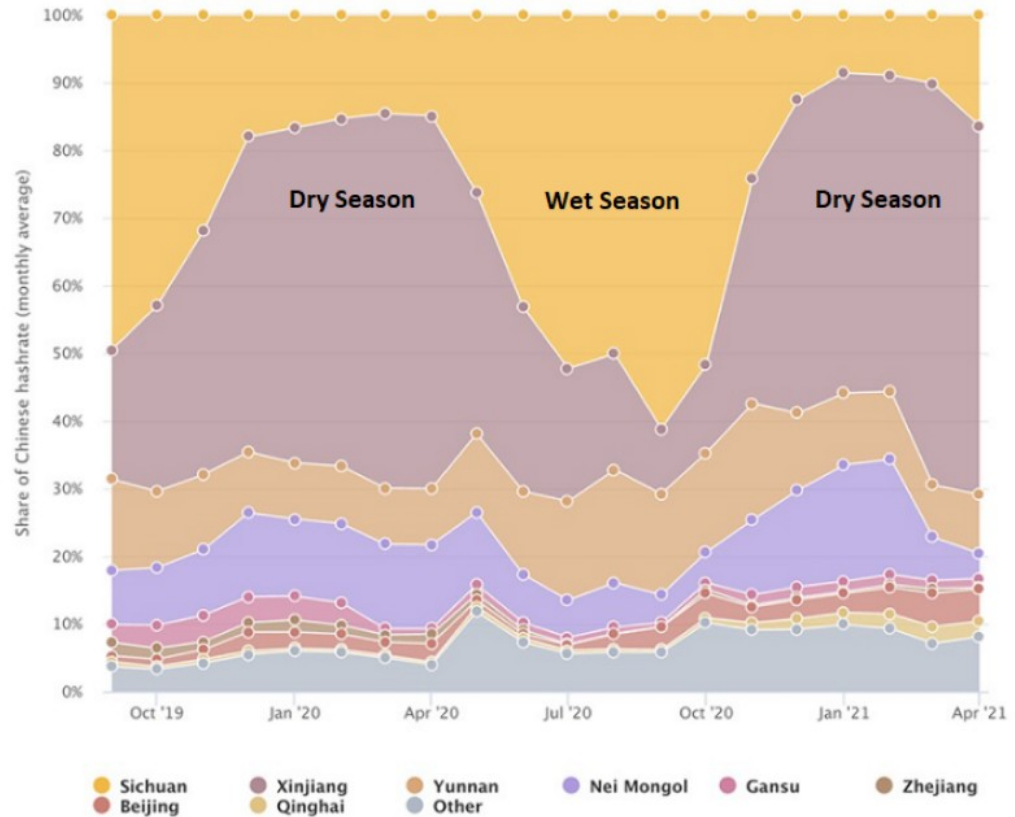


Chart Source: [University of Cambridge](#), Annotated by Lyn Alden

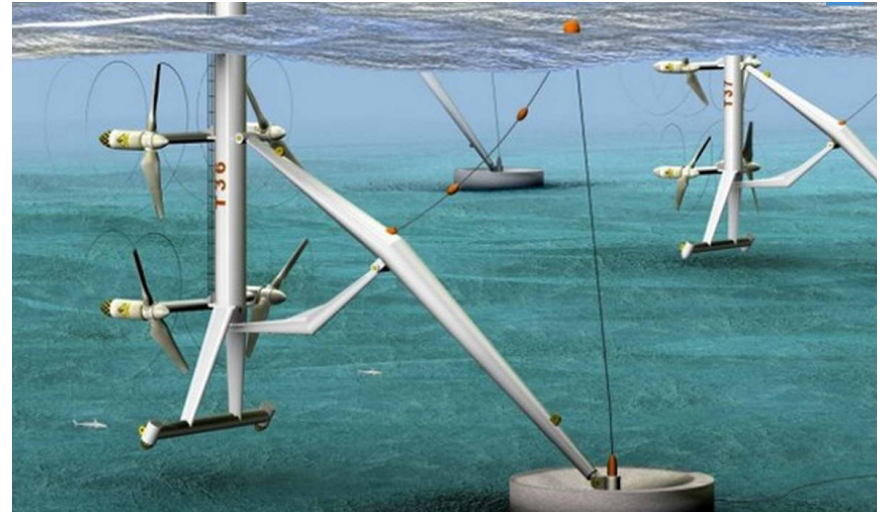
Ejemplos: reactores nucleares modulares (2/4)

- Reactores nucleares modulares (SMRs, CAREM)
- Oklo: empresa con licencia para construir y operar plantas nucleares en USA.
- Compass mining: empresa minera de bitcoin.
- El excedente de energía, puede usarse para minar, disminuyendo los costos de una instalación en una ciudad.
- Puede ayudar a resolver problemas de escala, si la ciudad consume menos que la energía del reactor.


Ejemplos: energía varada (3/4)

- Se puede empezar a generar energía, que se sabe económica, en una locación muy lejana a la red de distribución eléctrica.
- Minando, pueden conseguirse los fondos necesarios para conectar la fuente a la red de energía.
- El minado tiene capacidad de ser trasladado de una locación a otra.
- Los bitcoins obtenidos son convertibles a divisas de forma sencilla y segura.

Ejemplo: Energía Mareomotriz.
Península Valdez (?)



Ejemplos: uso eficiente de excedentes energéticos (4/4)

- Las redes de energía necesitan disponer de sobre-generación para ser robustas y responder a los picos de consumo.
 - Las fuentes renovables son intrínsecamente intermitentes (solar y eólica).
 - Puede minarse BTC, cuando no se utilice la energía extra y dejar de hacerlo, para responder a un pico.
- 

Bitcoin y Argentina



Puede Argentina utilizar esto a su favor?

- Minar en fuentes varadas.
- Bitcoin convierte energía barata en **dólares**.
- Optimizar costos de proyectos energéticos (CAREM (?)).
- Ayudar a financiar fuentes de generación y su conexión a la red troncal.
- Investigar y aplicar estas tecnologías

Vaca Muerta



CAREM



Muchas Gracias!

