

Los mineros son el poder ejecutivo de Bitcoin

Los mineros de Bitcoin están sometidos a los vaivenes del precio de mercado. Esto es cierto; pero también es cierto que -si lo deciden- pueden ignorar el beneficio a corto plazo. Esta capacidad los convierte en custodios de las propiedades monetarias de Bitcoin. Por lo tanto, cabe decir que los mineros tienen el poder ejecutivo en la *Blockchain*.

Los mineros pueden escribir -en proporción a su poder de cómputo- en la cadena de bloques de una red basada en *prueba de trabajo*. También -con el consenso suficiente- pueden escribir bloques vacíos legítimos en una cadena minoritaria con el fin de provocar su colapso. Y pueden hacer esto si juzgan que tal extremo resulta conveniente para la red y, por lo tanto, para sus intereses a largo plazo.

Los mineros pueden ejercer su poder en tiempo real, de forma ágil y eminentemente ejecutiva, registrando sus decisiones de forma públicamente verificable gracias al sistema de voto más seguro y fiable que se conoce.

Por lo tanto, los mineros mandan en Bitcoin. Y nunca actuarán en solitario porque juntos conforman una entidad de aliados sin conflicto de intereses (excepto en la competición por la potencia de cálculo).

Como nueva forma de poder ejecutivo que constituyen, es probable que en un futuro próximo se establezca un Parlamento Minero de Bitcoin (BMP) virtual y transparente donde cada participante tenga voz y voto en proporción a su porcentaje de *exahases* por segundo demostrables.

En este Parlamento alcanzarán acuerdos, se trazarán planes para resolver los futuros conflictos, se podrán nombrar portavoces o presidentes legítimos y se acelerará la selección de las mejores tecnologías de *Blockchain* ya probadas en la cantera de *altcoins*. Además, tendrán un contacto más preciso y cercano con la comunidad de usuarios y desarrolladores de Bitcoin.

Satoshi inventó deliberadamente el rol de los mineros porque el futuro de Bitcoin necesita ser confiado a una entidad superior a una sola persona o a un grupúsculo de desarrolladores.

Su existencia ha sido pensada para cumplir con un propósito y persistir en el tiempo. Son el contrapeso necesario para que la *Blockchain* pueda navegar a través del tiempo.

Su legítima recompensa son las tarifas correspondientes a todas las transacciones pasadas, presentes y futuras.

Su interés siempre será el mismo y, por lo tanto, su comportamiento seguirá un patrón predecible y estable en el tiempo.

Esto es la manifestación de lo que se conoce como El Consenso de Nakamoto.

Ignorar estos hechos dará lugar a una *Blockchain* quebradiza y con tendencia a la ruptura en cada controversia. Aceptar el mecanismo de consenso supone el empoderamiento de los mineros para que ostenten sobre la *Blockchain* su legítimo poder en su precisa magnitud.

Asimismo, aceptar esta realidad podría garantizar indefinidamente el cumplimiento de la última línea de la última página del *paper* original de Satoshi Nakamoto que dice así:

*“Cualesquiera reglas e incentivos necesarios
pueden ser aplicados con este mecanismo de consenso.”*

Javier González González

GONZO@virtualpol.com

[@JavierGonzalez](#)

1AAtd721LQekC6ncHbAp4ScKxSwR7fFeYT BCH

2017-10-31

[ES](#) [EN](#)

Referencia

1. Satoshi Nakamoto, 2008-10-31.
[“Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer”](#)

Anexo I

Mapa con las claves del conflicto del 2017:

	Bitcoin Core	Bitcoin Cash
Is it Bitcoin?	Yes	No
Is it the most powerful?		
Is it the safest?		
Is the longest blockchain?		
Transaction cost?	Expensive or unpredictable	Always cheap
Transaction speed?	Slower frequently	Predictable and fast
Respect the original design?	No	Yes
Who approves the solutions?	Some developers	Miners (with hashpower)
Solutions type?	Off-chain	On-chain
Future scaling solutions?	Ligthining Network?	Sharding? Block frequency?
Block limit?	1MB	Unlimited
Transactions per second?	5	
Maleability fix?	Segwit, when used	In development (MalFix?)
Weak to empty block attacks?	Yes	No
Non-mining nodes define something?	No	No
Are there enough nodes deployed?	Yes	Yes
Identifiers?	XBT BTC	BCH BCC

2017-10-31 v4 @JavierGonzalez

Anexo II

Escenario hipotético de la situación a corto plazo.

Pronto, el NYA (Acuerdo de Nueva York) se extinguirá y los mineros tendrán tres opciones:

- 1) No hacer nada y ceder la toma de decisiones a un equipo vertical y autoritario de desarrolladores a quienes les gustan los *takeovers* y la censura, incapaces de desarrollar soluciones *on-chain* porque están enfocados en apropiarse de las futuras tarifas cuyos legítimos herederos son los mineros; precisamente, el hecho de que estas tarifas correspondan legítimamente a los mineros constituye el único incentivo a largo plazo para costear la seguridad de todo el proyecto Bitcoin.
En lugar de asumir la arquitectura original de Satoshi, se ha llegado al extremo de estrangular artificialmente la tasa de transacciones por segundo provocando con ello un retroceso en la aceptación de Bitcoin, aceptación que es la base del valor de Bitcoin. Y esto se ha ejecutado, simplemente, para hacer necesaria mediante el chantaje, su solución privada.
- 2) Hacer un tercer *hard fork* y así subdividir nuevamente a la comunidad en una tercera parte, desarrollar nuevos clientes, desplegar cientos de nodos (que necesitarían de una próxima ampliación), empezar la campaña desde cero y todo esto tan solo para, simplemente, aplazar el conflicto.
- 3) Dirigir el *hashpower* a Bitcoin Cash y hacer valer El Consenso de Nakamoto, logrando así que Bitcoin Cash sea -además de rápido y barato- también el más seguro, con más “prueba de trabajo”, y, por tanto, digno de ser llamado Bitcoin. Igualmente, habría que contemplar la posibilidad de, si es necesario, minar bloques vacíos en la *Blockchain* minoritaria para reducir riesgos y que quede claro quien manda.

Anexo III

Características predecibles de los mineros como entidad (no aplicables a nivel individual):

- Prudentes

Los mineros tienen una importante y permanente inversión en *hardware* que solo sirve para minar Bitcoin.

Su prudencia está a otro nivel nunca visto.

Pensarán siempre a largo plazo. Medirán mejor que nadie los riesgos de cada decisión. Preferirán los hechos a las palabras. Nunca actuarán de forma improvisada o precipitada.

- Competentes

Son los supervivientes de una carrera tecnológica tan competitiva que podría quebrantar la *Ley de Moore*. Su nivel técnico solo puede estar al día.

- Cumplidores de su palabra

Nadie quiere alcanzar acuerdos con quien se desdice, por ello los mineros cumplirán lo que prometen. No adquirirán compromisos que no puedan cumplir con seguridad.

Han cumplido su parte del NYA y la propia *Blockchain* es la mejor prueba de su fiabilidad.

Son capaces de esperar hasta que el acuerdo NYA se extinga en noviembre -pese a estar dañando la aceptación de Bitcoin- solo para que nadie les pueda acusar de haber incumplido su palabra.

- Diplomáticos

Sólo ganan unidos. Por lo tanto, buscarán siempre el consenso.

Han tendido la mano con *Segwit2X* como término medio de *paz*, a pesar de ceder poder y tan solo aplazar el problema.

Esto ha sido un acto de generosidad a cambio de cierta estabilidad que ellos saben valorar mejor que nadie.

- Precisos

Un error en la *Blockchain* podría ser fatal.

Un error de comprensión o de estrategia les dejaría fuera de juego.

Incluso una mala jugada no letal es algo inaceptable para los mineros.

- Capaces

Son capaces de mantener la infraestructura necesaria con un creciente presupuesto.

Y de desarrollar *software* incluso con varios equipos.

Podrán mantener suficientes nodos y de cualquier tamaño con la ayuda de la *Ley de Moore*.

- Confiables

Están interesados en su propio beneficio, pero su beneficio propio está inherentemente alineado con el bienestar y continuidad de Bitcoin en el futuro. Así lo programó Satoshi y en ese objetivo común coincidimos todos.

Anexo IV

Contra-argumentario de las objeciones más frecuentes:

- *Satoshi puso el límite de 1MB.*

Lo hizo como contramedida de seguridad temporal, cuando la media por bloque era de unos pocos kilobytes y no se llenaban. Inaceptablemente, algunos han visto aquí su oportunidad para legitimar la estrangulación de la capacidad de la red.

- *El diseño original de Bitcoin no escala.*

La *Blockchain* actual tiene un tamaño de 140 GB. Existen servidores con 36 bahías de 3.5" y discos de 12 TB. Así, podemos almacenar 430 TB en una sola máquina, pudiendo almacenar la *Blockchain* 3.071 veces a día de hoy. La *Ley de Moore* es una mera observación, pero se cumple. Y dice que cada 2 años se duplica la capacidad. Así se estima que en 2020 cada *supernodo* podrá almacenar 6.034 veces la *Blockchain* actual y en 2030 unas 193.088 veces (27 PB). La *Ley de Moore* también es aplicable al ancho de banda, latencia, lecturas en disco y potencia de cálculo. Además, sin ser necesario, existen otras opciones como los *mainframes* (grandes ordenadores no convencionales), los sistemas distribuidos (*clusters*) y la computación *cloud*.

Y todo esto sin contar con que probablemente los desarrolladores centrados en soluciones *on-chain* encontrarán optimizaciones y estrategias para escalar cuando y cuanto sea necesario.

- *La minería es un monopolio de una sola empresa.*

Existen dos fabricantes de GPU y unos pocos más de CPU. La distribución es proporcional al tamaño de cada mercado. Todo lo necesario para practicar la minería es de dominio público y no existe ninguna barrera que impida la libre competencia. Es previsible que con el tiempo aumentará el número de fabricantes de chips ASIC competitivos.

- *Segwit ya supone un aumento del límite de bloque.*

Es verdad, pero el aumento en la práctica es insignificante.

- *Bitcoin Cash es una altcoin.*

Bitcoin Cash respeta el diseño original. Bitcoin Core en algún momento decidió modificar sustancialmente el diseño original. En adelante, esto debe hacerse siempre en una *altcoin*.

- *Los mineros necesitan que los nodos acepten su Blockchain.*

El desarrollo y despliegue de nodos que no minan es barato y está al alcance de los mineros. Los nodos solo confirman, nunca rechazan transacciones, porque pueden ser ignoradas. Por lo tanto, los nodos no tienen ningún poder.

- *El equipo de desarrollo de Bitcoin Core es meritocrático.*

Las redes de IRC, foros, blogs y redes sociales se vertebran con una jerarquía vertical. Son la forma de autoritarismo más puro, donde el fundador -el primero en llegar- por sí mismo tiene el poder absoluto y es irrevocable. Este primitivo sistema de toma de decisiones -ante controversias- tiende a degenerar en despotismo, censura y la expulsión de los participantes discordantes siendo la antítesis del comportamiento de los mineros.

Esto daña la diversidad, crea *cavernas* de opinión y fractura la comunidad.

La solución es que varios equipos de desarrolladores compitan.

- *Con nodos pequeños Bitcoin es más democrático o descentralizado.*

Bitcoin no es democrático (idealizaciones aparte). Se impide el doble gasto, pero no el doble voto. Además, este esquema estaría basado en las direcciones IP que son muy baratas. Los nodos que no minan no tienen ningún poder sobre la Blockchain, así que su número, tamaño y ubicación es irrelevante.

- *Los desarrolladores pueden cambiar a un algoritmo resistente a chips ASIC.*

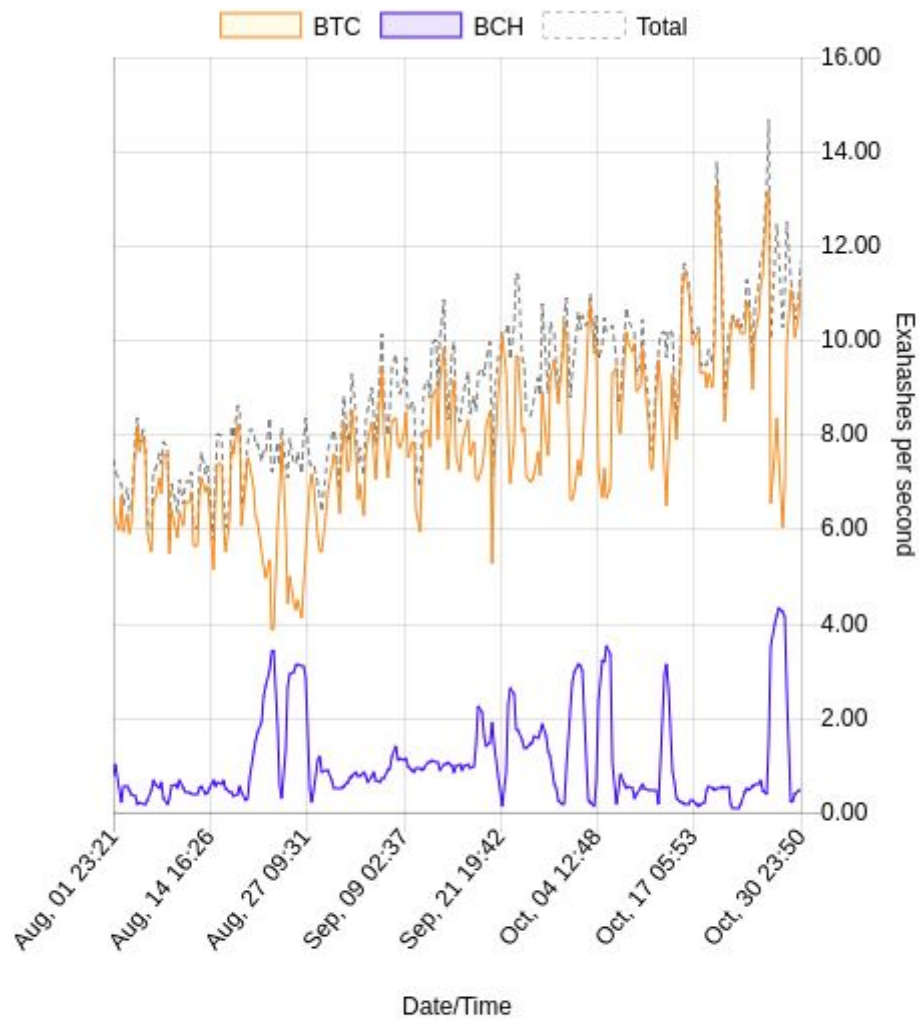
Pueden hacerlo, pero eso no sería Bitcoin. Es muy arriesgado e implica un nuevo *hard fork*. Es cuestión de tiempo que alguien fabrique chips específicos para cualquier algoritmo, lo cual implica sucesivos cambios arbitrarios decididos probablemente por un equipo vertical y autoritario de desarrolladores en contra de su propia comunidad minera.

Por lo tanto, cambiar unos mineros por otros no resuelve nada porque implica regresar cíclicamente al empoderamiento minero.

Anexo V

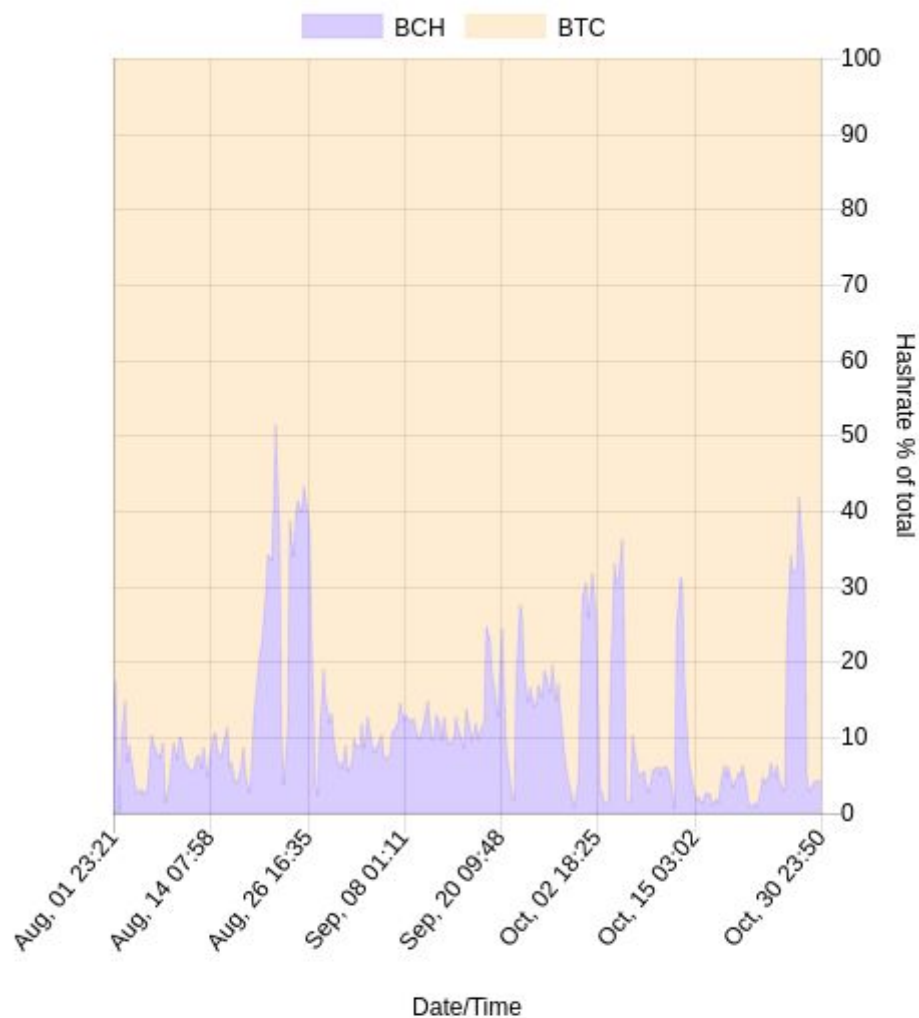
Hechos relacionados:

Absolute hashrate in exahashes per second (12h averages).



Coin	3h	12h	1d	3d	7d
BTC	16.76	11.27	10.62	9.36	9.62
BCH	0.72	0.47	0.43	1.83	1.67

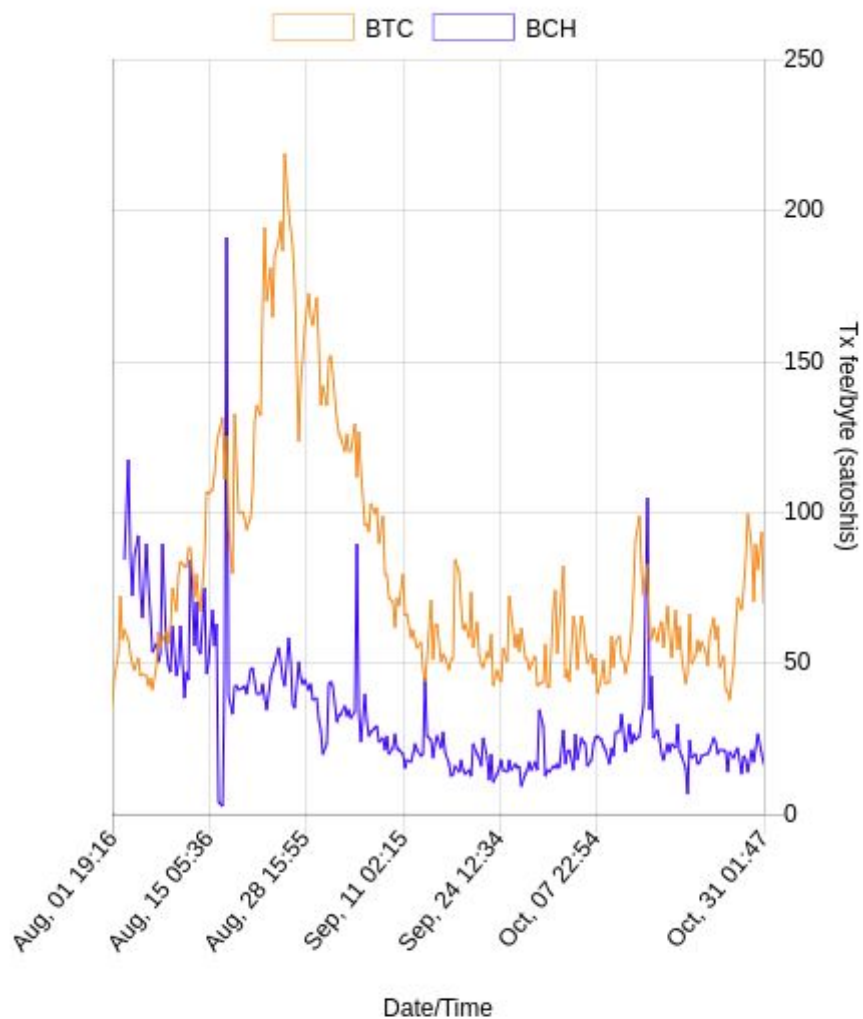
Relative hashrate in percentage of total (stacked, 3h averages).



Disclaimer: Please note that using a 3 hour average is not the most reliable way of measuring this data. This data should be interpreted as an estimate. The real number can differ by several percent.

Coin	3h	12h	1d	3d	7d
BTC	95.88%	95.98%	96.15%	83.65%	85.18%
BCH	4.12%	4.02%	3.85%	16.35%	14.82%

Average tx fee in satoshis per byte.



Note: these statistics show fees for the average tx size. For regular transactions (with few inputs/outputs) the median tx size is a more useful statistic but that data is currently not available.

Coin	3h	6h	12h	1d	7d
BTC	71.74	75.51	83.43	82.15	65.91
BCH	15.45	17.70	18.78	21.50	19.28

Fuente: fork.io/

BLOCK SUMMARY

Blocks Mined	145
Time Between Blocks	9.4 minutes
Bitcoins Mined	1,812.50000000 BTC

MARKET SUMMARY

Market Price	\$6,105.93
Trade Volume	\$411,984,646.91
Trade Volume	67,547.84000000 BTC

TRANSACTION SUMMARY

Total Transaction Fees (BTC)	263.61686670 BTC
Number of Transactions	312,595
Total Output Volume (BTC)	1,860,676.52351116 BTC
Estimated Transaction Volume (BTC)	270,036.00811345 BTC
Estimated Transaction Volume (USD)	\$1,646,991,019.00











MINING COST

Total Miners Revenue (USD)	\$12,662,555.10
% Earned From Transaction Fees	12.71%
% Of Transaction Volume	0.77%
Cost per Transaction (USD)	\$40.55

HASH RATE AND ELECTRICITY CONSUMPTION

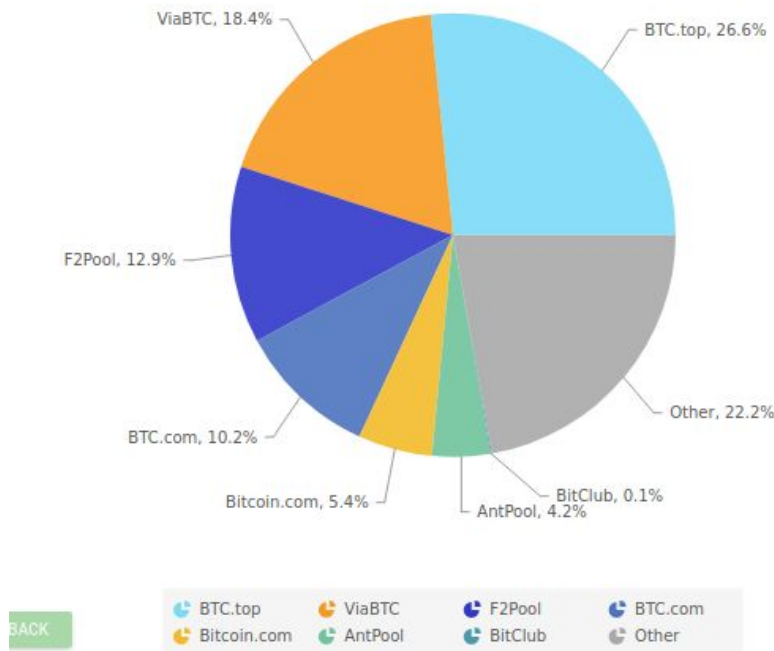
Difficulty	1,452,839,779,145
Hash Rate	10,472,053,287 GH/s

Fuente: [Blockchain.info](https://blockchain.info)

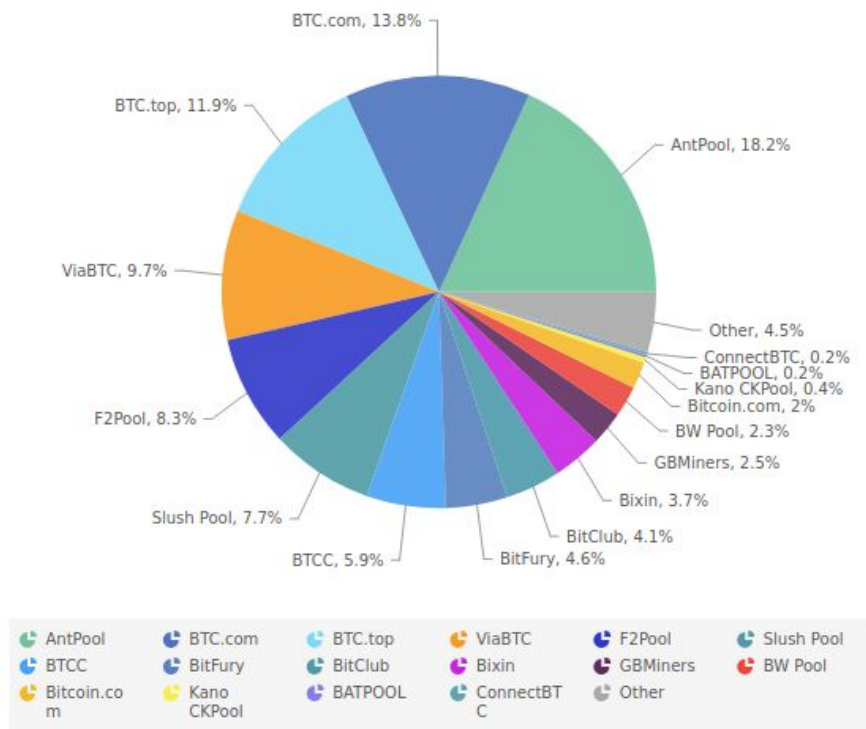
MARKET SHARE			
TOTAL: \$182,517,287,992			
CURRENCY	PRICE	MARKET CAP	MARKET SHARE
BITCOIN 	\$6393.34	<u>\$106,490,744,430</u>	<u>58.35%</u>
ETHEREUM 	\$307.70	<u>\$29,367,013,714</u>	<u>16.09%</u>
RIPPLE 	\$0.20	\$7,784,989,187	<u>4.27%</u>
BITCOIN CASH 	\$449.97	\$7,537,577,081	4.13%
LITECOIN 	\$56.36	\$3,021,854,179	1.66%
DASH 	\$283.93	\$2,173,382,607	1.19%
NEO 	\$28.86	\$1,875,984,500	1.03%
NEM 	\$0.19	\$1,734,291,000	0.95%
BITCONNECT 	\$236.32	\$1,734,248,814	0.95%
MONERO 	\$88.38	\$1,351,493,474	0.74%

Fuente: flipping.watch

Latest Bitcoin Cash Blocks by Mining Pool (last 1000 blocks)
coin.dance



Latest Bitcoin Blocks by Mining Pool (last 7 days)
coin.dance




Fuente: coin.dance

Anexo VI

Carta abierta que escribí el 25 de Marzo del 2017 publicada en *Bitcointalk* y *Reddit*:

Topic: Dear Bitcoin Miners (Read 1135 times)

 **Dear Bitcoin Miners**
March 25, 2017, 06:27:50 PM

Dear Bitcoin Miners:

I ask you please to defend your interests now.

Satoshi invented Bitcoin based only on proof-of-work.
You have control of the computing power.
Therefore, the correct functioning and future of Bitcoin depends on you.

Satoshi knew this would happen and decided to trust you because he assumed that you would always act for the benefit of your own interest.
Commissions of transactions - past, present and future - belong to you.

The developers, nodes, markets and the media do not have the control of the blockchain.
Only you can determine which is the real blockchain.

You have a great investment and a promising future.
But you have machines that only serve for this purpose.
If you do not do the right thing soon you will turn off the machines so as not to go bankrupt because of the high energy consumption and you will lose everything.

IMHO I suggest the following plan:

1. Hold meetings of miners in private (the same interests).
2. You must reach a consensus of a Mining Alliance of +75% to solve this crisis (zero-sum game).
3. Announce and consolidate that alliance in the text associated with the blocks.
4. Coordinate and compensate between you to neutralize the incorrect blockchain (hard is hard).
5. Acting forcefully, quickly and always in your own interest.

The great catastrophe is moving fast.
Please, do it now.

Sincerely,

Fuentes: reddit.com/r/Bitcoin y bitcointalk.org (archive.org)