El Parlamento Minero de Bitcoin

Extracto. *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.*

Los mineros son el poder ejecutivo de Bitcoin 2017-10-31

Actualmente, los mineros de Bitcoin estiman el consenso con inadecuada coordinación.

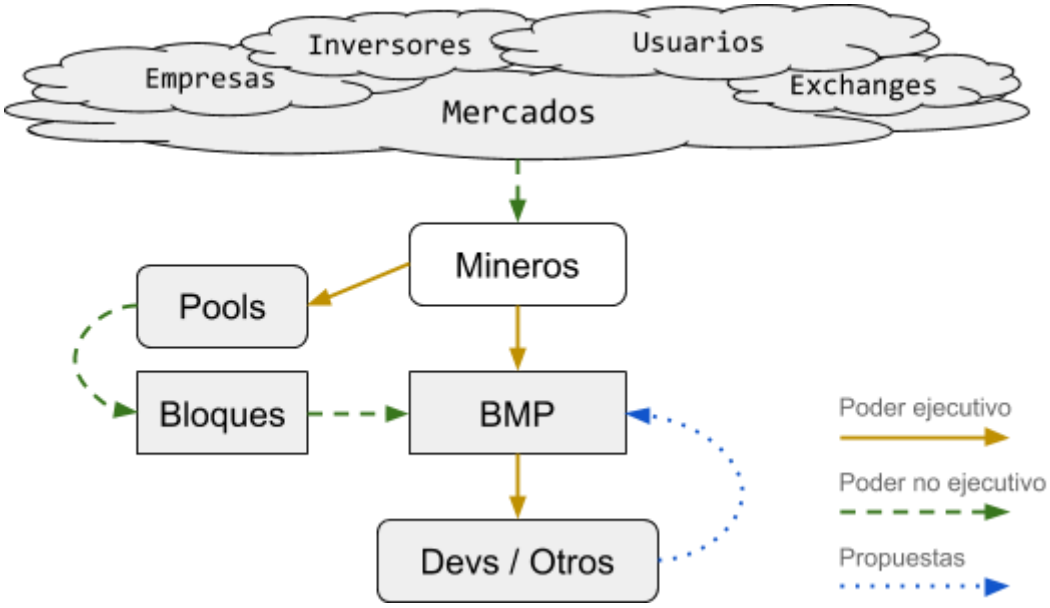
Esto provoca *hardforks* contenciosos que dividen la *blockchain*, fracturan la comunidad, generan confusión y dañan la adopción. Los mineros pueden asumir, mejor que nadie, la responsabilidad de prevenir el riesgo de que tales eventos se repitan.

En el proceso de desarrollo tecnológico, con frecuencia, surgen encrucijadas con dos soluciones válidas pero incompatibles en la misma *blockchain*. Por lo tanto, el desarrollo tecnológico exige la toma decisiones.

La tendencia humana a enredarse en conflictos es un patrón previsible. Con múltiples equipos de desarrollo compitiendo, la confrontación es solo cuestión de tiempo. Para resolver esto, los mineros deben desempeñar su rol ejecutivo.

Además, en una carrera tecnológica el vector de aceleración es un factor decisivo que marca la diferencia. La adopción global será conquistada por la *blockchain* capaz de evolucionar tecnológicamente a mayor velocidad.

Para que una adopción global exitosa sea posible, los mineros de Bitcoin deben coordinarse eficazmente.



Votando con potencia de cálculo (*hashpower*), los mineros pueden actuar como una entidad.

Coordinados, como si de un *General Bizantino virtual* se tratase, los mineros pueden llegar a un consenso legítimo que sea reconocido como la voz de los mineros de Bitcoin. El impacto de sus decisiones, buenas o malas, recaerá plenamente sobre ellos.

La legitimidad es un requisito indispensable para que el Parlamento Minero de Bitcoin (BMP) sea vinculante. Esto se consigue con una clara verificabilidad, que emanará directamente de los bloques de la *blockchain*.

Los *pools* solo son representantes temporales del *hashpower* aportado por quien decide minar con ellos para crear bloques. Pueden ser reemplazados sin riesgo y con facilidad. Por lo tanto, no tienen poder ejecutivo. Los mineros tienen el poder ejecutivo, porque son quienes controlan máquinas de minería y costean la electricidad.

En la transacción *coinbase* de cada bloque, los *pools* deberán publicar las *direcciones* de los principales mineros en múltiples *outputs*, indicando en el *OP_RETURN* el porcentaje de *hashpower* correspondiente a cada minero.

```
Descripción         Hexadecimal
OP_RETURN           0x6a
Reserved prefix     0x9d01
Value [1,10000]     0x2710       (10000 = 100,00%)

OP_RETURN 9d01 4d2               (12,34%)
OP_RETURN 9d01 1a0a              (66,66%)
```

El *hashpower* individual de cada minero se calcula en función de su cuota señalizada a partir del *hashpower* registrado en el bloque. Un *pool* nunca podrá controlar más *hashpower* que el demostrado en sus bloques.

Así, cada minero podrá demostrar su esfuerzo, más allá de la *blockchain*, en proporción a su porcentaje de *hashpower*.

La implementación de esta señalización depende de la voluntad de los mineros. Esta voluntad puede expresarse mediante la transferencia del *hashpower* a los *pools* que publiquen en cada bloque esta información con precisión.

El BMP será vinculante cuando participe la mayor parte del *hashpower*.

El Parlamento Minero de Bitcoin se puede implementar de diversas formas.
Expondré una de ellas, la más avanzada según mi criterio y experiencia:

- No es necesario alterar el protocolo de la *blockchain*, ni las operaciones de minería.
- El espacio debe ser virtual -a través de internet- para poder representar el máximo porcentaje posible de *hashpower*.
- Idealmente, la base de datos puede ser *on-chain*, pero en algún punto tendrá que funcionar en un servidor web. El requisito fundamental es que la legitimidad tenga su raíz en la *blockchain* y, por lo tanto, sea universalmente verificable.
- La transparencia facilitará la verificabilidad y la comprensión de las decisiones por parte de la comunidad de usuarios.
- El sistema base consta de un registro de usuarios, los cuales podrán reclamar su cuota de *hashpower* asociado a una o más direcciones de Bitcoin. Lo harán aportando una firma que demuestre el control de cada dirección. Haciendo pública esta información, con la tecnología adecuada, los mineros de Bitcoin podrán demostrar la cantidad de *hashpower* que controlan, más allá de la *blockchain*.
- El *hashpower* de cada minero se presentará indicando la cantidad de *hashes* por segundo y el porcentaje correspondiente a la proporción directa de su *hashpower* frente al total registrado en la *blockchain* (Ver Anexo V).
- En el mismo espacio, mediante los medios de comunicación típicos de internet (chats, foros, mensajes, etc), los mineros podrán debatir, deliberar y finalmente crear propuestas de votaciones para obtener información o tomar decisiones vinculantes.

Así, los mineros podrán realizar votaciones actuando con su porcentaje de *hashpower*. Tras el resultado, la opción en mayoría sería legítimamente representativa de los mineros de Bitcoin, respetando en todo momento el *whitepaper* de Satoshi Nakamoto.

> ***Extracto.*** *Votan con su potencia CPU, expresando su aceptación de los bloques válidos trabajando en extenderlos y descartando los bloques no válidos al rechazar trabajar en ellos. Cualesquiera reglas e incentivos necesarios pueden ser aplicados con este mecanismo de consenso.*
>
> *Bitcoin: un sistema de dinero en efectivo electrónico 2008-10-31*

Javier González González
@JavierGonzalez
15bdKu8Wfiyie3xP4jVxTNo9KThCeQkiZd (BCH)
2018-06-15
ES EN CN

Anexo I

Contra-argumentario a las objeciones más frecuentes:

1. *Será el principio de un gobierno o estado autoritario.*

Los mineros no están interesados en planificar la vida de los demás.
Persiguen individualmente su propio interés, que está alineado con el bienestar futuro de Bitcoin valorado por los mercados.

- Si los mineros actúan mal, bajará el precio de mercado.
- Si los *pools* se apropian indebidamente del *hashpower*, serán reemplazados.
- Si el BMP no es verificable, será reemplazado.
- Si la mayoría del *hashpower* no actúa coordinadamente, habrá otro *hardfork* contencioso.

2. *Bitcoin funciona perfectamente con hardforks.*

El *whitepaper* de Satoshi Nakamoto establece un mecanismo de resolución de conflictos que funciona. Pero no es deseable. Daña la adopción. Este recurso debe ser usado solo en última instancia y cuando no quede otra alternativa.

3. *Implica coacción, con imposiciones no voluntarias.*

Para que el incentivo de un minero sea efectivo, no basta con ser el primero en publicar el siguiente bloque válido. También es necesario que los dueños de la mayor parte del *hashpower* decidan voluntariamente trabajar para continuar exactamente ese bloque.
Es un consenso, sin coacción, totalmente legítimo.

4. *No funcionará mejor que el mercado.*

Nadie es mejor que los mineros para tomar decisiones sobre sus propios negocios.

5. *No se puede representar el 100% del hashpower.*

Es cierto, pero es fácil representar la mayor parte del *hashpower*.
Dividiendo el *hashpower* total en solo 100 participantes, se podría representar el 97,9% del *hashpower* SHA256 (Anexo III) con 16 *pools*, incluidos 6 participantes correspondientes a *hashpower* desconocido.
Esta limitación técnica-operativa se puede mitigar elevando el consenso necesario para tomar decisiones más allá del 51%.

6. *El BMP es vulnerable.*

El origen de la legitimidad del BMP es la *blockchain*. Toda o parte de la información operativa se pueden almacenar *on-chain*. No puede afectar el normal funcionamiento de Bitcoin.

7. *Los mineros no son el poder ejecutivo de Bitcoin.*

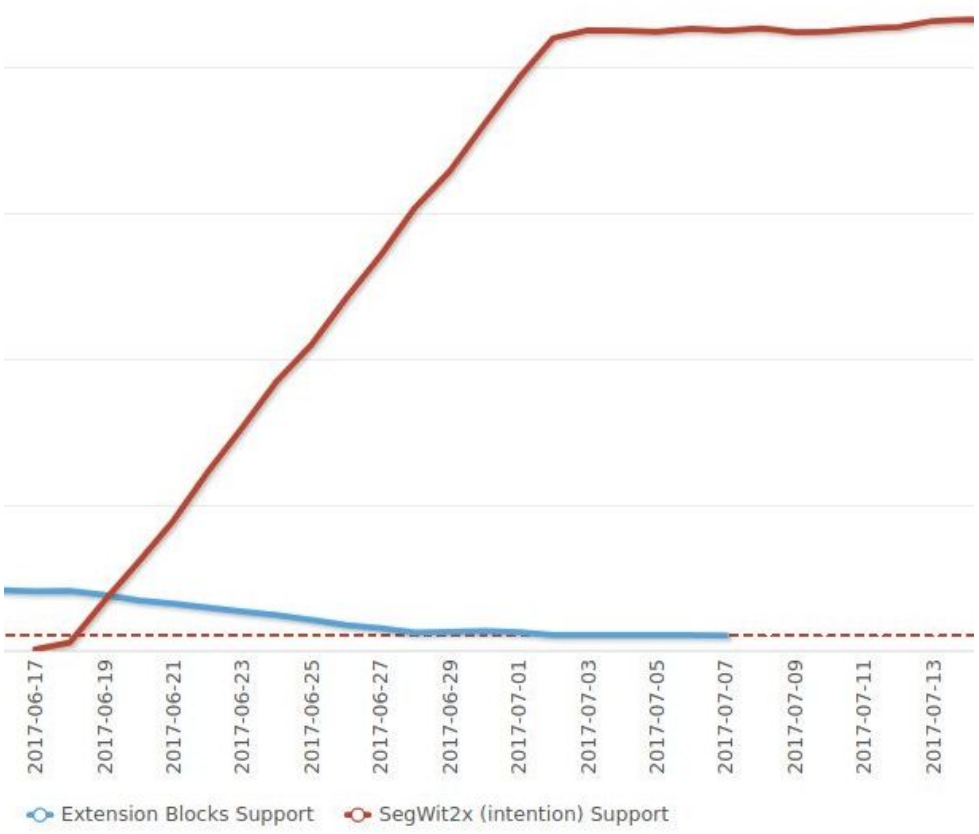
Los usuarios, a través de los nodos que no minan, no tienen ningún poder.
Los usuarios, a través de los mercados, tienen mucho poder. Es el mayor poder a medio y largo plazo, que prevalecerá sobre cualquier otro. Pero no es ejecutivo. No actúa, reacciona. Influye, pero indirectamente.
Los desarrolladores proponen las reglas de consenso, pero la decisión última se hace cumplir con *hashpower*.
Los mineros son competitivos, tienen todo el incentivo, controlan totalmente la *blockchain* y disponen del sistema de voto más seguro que existe.
Por lo tanto, los mineros no tienen el poder absoluto, pero el poder ejecutivo, con las responsabilidades que ello implica.

Anexo II

Informalmente, los mineros de Bitcoin ya existen como entidad.

El 19 de junio del 2017, el 85% del *hashpower* señalizó /NYA/ en la *blockchain* de forma estable durante 5 meses. Este evento ocurrió prácticamente al unísono evidenciando una coordinación previa en torno a una fecha objetivo.

La descoordinación no hace líneas rectas.



Fuente: [coin.dance]

Anexo III

	Bitcoin		Bitcoin Cash		Bitcoin Core	
	100%	39.770 PH/s	12%	4.960 PH/s	88%	34.810 PH/s
Pools	**Power**	**Hashpower**	**Power**	**Hashpower**	**Power**	**Hashpower**
BTC.com	24,7%	9.819 PH/s	8,9%	439 PH/s	26,9%	9.380 PH/s
AntPool	12,9%	5.150 PH/s	8,7%	430 PH/s	13,6%	4.720 PH/s
BTC.TOP	10,5%	4.176 PH/s	20,1%	996 PH/s	9,1%	3.180 PH/s
ViaBTC	10,4%	4.127 PH/s	19,1%	947 PH/s	9,1%	3.180 PH/s
SlushPool	10,0%	3.990 PH/s			11,5%	3.990 PH/s
F2Pool	7,8%	3.110 PH/s			8,9%	3.110 PH/s
Unknow	6,0%	2.397 PH/s	29,1%	1.445 PH/s	2,7%	952 PH/s
DPOOL	3,2%	1.260 PH/s			3,6%	1.260 PH/s
BTCC	2,2%	875 PH/s			2,5%	875 PH/s
Bixin	2,1%	840 PH/s			2,4%	840 PH/s
BW.COM	1,8%	735 PH/s			2,1%	735 PH/s
BitFury	1,8%	700 PH/s			2,0%	700 PH/s
Bitcoin.com	1,6%	626 PH/s	7,0%	347 PH/s	0,8%	280 PH/s
BTPOOL	1,1%	455 PH/s			1,3%	455 PH/s
BitClub	1,0%	385 PH/s			1,1%	385 PH/s
Huobi.pool	0,7%	277 PH/s	2,1%	103 PH/s	0,5%	175 PH/s
KanoPool	0,4%	175 PH/s			0,5%	175 PH/s
CanoePool	0,4%	140 PH/s			0,4%	140 PH/s
SBI Crypto	0,3%	112 PH/s	2,3%	112 PH/s		
CKPool	0,3%	105 PH/s			0,3%	105 PH/s
WAYI.CN	0,2%	98 PH/s	2,0%	98 PH/s		
58COIN	0,2%	70 PH/s			0,2%	70 PH/s
ConnectBTC	0,2%	70 PH/s			0,2%	70 PH/s
Waterhole	0,1%	44 PH/s	0,9%	44 PH/s		
BitcoinRussia	0,1%	35 PH/s			0,1%	35 PH/s

Anexo IV

Los mineros, como entidad, pueden hablar.

Del mismo modo que eligen por consenso cuál es el siguiente bloque de la *blockchain*, con el sistema adecuado, los mineros podrán proponer mensajes y decidir votando cuál es el siguiente mensaje, en el contexto de una conversación.

La conversación puede ser entre la entidad y un individuo, pero también de la entidad consigo misma, respondiendo a sus propios mensajes, deliberando y estableciendo en el proceso una opinión propia, unificada y representativa -con el *hashpower* como conductor- de la inteligencia colectiva de los mineros, en el contexto de una reunión.

Anexo V

Maquetas de ejemplo.