

The Bitcoin Mining Parliament

Extract. As a new form of executive power, it is likely that in the near future a virtual and transparent Bitcoin Mining Parliament (BMP) will be established. There each participant can have voice and vote in proportion to their percentage of demonstrable exahases per second.

[Miners are the executive power of Bitcoin](#) 2017-10-31

Currently, the Bitcoin miners estimate consensus with inadequate coordination.

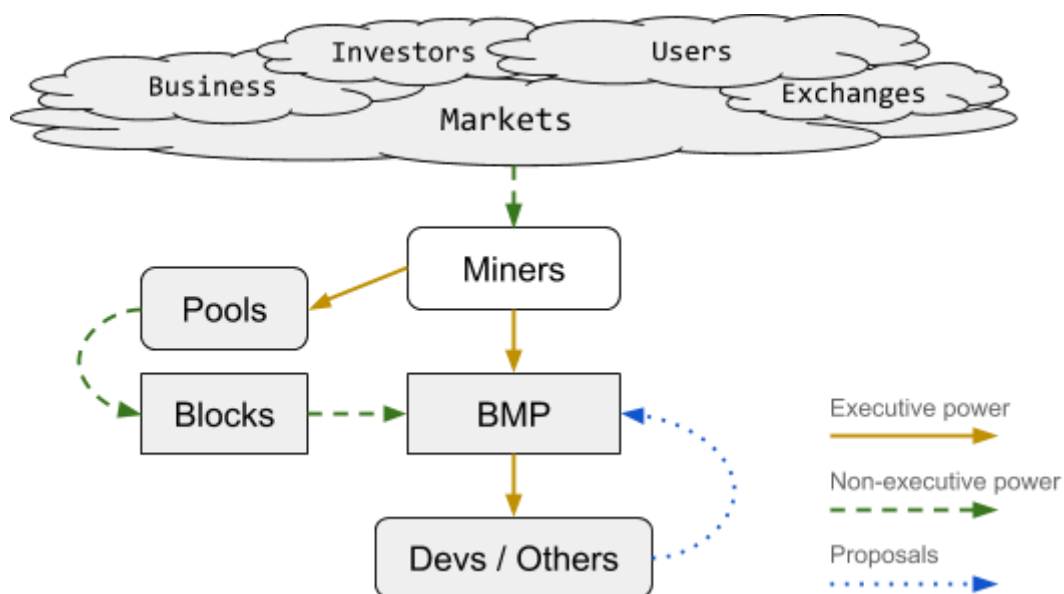
This causes contentious hardforks that divide the *blockchain*, fracture the community, create confusion and damage adoption. Miners can take responsibility, better than anyone else, for preventing the risk of such events happening again.

In the process of technological development, often crossroads arise with two valid but incompatible solutions in the same *blockchain*. Therefore, technological development requires decision-making.

The human tendency to become entangled in conflict is a predictable pattern. With multiple development teams competing, confrontation is only a matter of time. To resolve this, miners must assume their executive role.

Moreover, in a technological race, the acceleration vector is a decisive factor that makes the difference. Global adoption will be conquered by the *blockchain* capable of evolving technologically at a faster rate.

For a successful global adoption to be possible, Bitcoin miners must coordinate effectively.



Voting with computational power (*hashpower*), miners can act as an entity.

Coordinated, as if it were a *virtual Byzantine General*, the miners can reach a legitimate consensus that is recognized as the voice of the Bitcoin miners. The impact of their decisions, good or bad, will fall fully on them.

Users, through non-mining nodes, have zero power.

Users, through the markets, have a lot of power. It is the greatest power in the medium and long term, which will prevail over all others. But it's not executive. It doesn't act, it reacts. Influences, but indirectly.

The developers propose the rules of consensus, but the ultimate decision is enforced with *hashpower*. The miners are competitive, they have all the incentive, they totally control the *blockchain* and they have the most secure voting system that exists.

Therefore, the miners do not have absolute power, but they do have executive power, with the responsibilities that this implies.

Legitimacy is a pre-requisite for the Bitcoin Mining Parliament (BMP) to be binding. This is achieved with a clear verifiability, which will emanate directly from the blocks of the *blockchain*.

The *pools* are only temporary representatives of the *hashpower* contributed by the one who decides to mine with them to create blocks. They can be replaced without risk and with facility. Therefore, they have no executive power. The miners have executive power, because they control mining machines and finance electricity.

In the *coinbase* transaction of each block, the *pools* must publish the *addresses* of the main miners in multiple *outputs*, indicating in the *OP_RETURN* the percentage of *hashpower* corresponding to each miner.

Description	Hexadecimal	
OP_RETURN	0x6a	
Reserved prefix	0x9d01	
Value [1,10000]	0x2710	(10000 = 100.00%)

The individual *hashpower* of each miner is calculated with his quota signalled with the *hashpower* registered in the block. A *pool* will never be able to control more *hashpower* than that demonstrated in its blocks.

In this way, each miner will be able to demonstrate his effort, beyond the *blockchain*, in proportion to his percentage of *hashpower*.

The implementation of this signalization depends on the will of the miners. This will can be expressed through the transfer of the *hashpower* to the *pools* that publish this information in each block with precision.

The BMP will be binding when most of the *hashpower* is participating.

The Bitcoin Mining Parliament can be implemented in a diversity of forms.
I will present one of them, the most advanced in my opinion and experience:

- There is no need to alter the *blockchain* protocol or mining operations.
- The space must be virtual -via Internet- in order to represent the maximum possible percentage of *hashpower*.
- Ideally, the database can be on-chain, but at some point it will have to run on a web server. The fundamental requirement is that legitimacy must be firmly rooted in *blockchain* and therefore be universally verifiable.
- Transparency will facilitate the verifiability and understanding of decisions by the user community.
- The base system consists of a register of users, who can claim their *hashpower* quota associated with one or more Bitcoin *addresses*. They will do so by providing a signature demonstrating control of each *address*. By making this information public, with the right technology, Bitcoin miners will be able to demonstrate the amount of *hashpower* they control, beyond the *blockchain*.
- The *hashpower* of each miner will be presented indicating the number of hashes per second and the percentage corresponding to the direct proportion of his *hashpower* to the total registered in the *blockchain* (See Annex V).
- In the same space, through the typical Internet communication media (chats, forums, messages, etc), miners will be able to debate, deliberate and finally create voting proposals to obtain information or make binding decisions.

In this way, miners will be able to vote with their percentage of *hashpower*. After the result, the majority option would be legitimately representative of the Bitcoin miners, while respecting Satoshi Nakamoto's *whitepaper* at all times.

Extract. *They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.*

[Bitcoin: A Peer-to-Peer Electronic Cash System](#) 2008-10-31

Javier González González

[@JavierGonzalez](#)

15bdKu8Wfiyie3xP4jVxTNo9KThCeQkiZd (BCH)

2018-06-15

[ES EN CN](#)

Annex I

Counter-argumentary to the most frequent objections:

1. It will be the beginning of an authoritarian government or state.

Miners are not interested in planning the lives of other people.

They pursue their own individual interests, which are aligned with the future well-being of Bitcoin as valued by the markets.

- If the miners act badly, the market price will fall.
- If *pools* misappropriate *hashpower*, they will be replaced.
- If the BMP is not verifiable, will be replaced.
- If most *hashpower* does not act in a coordinated manner, there will be another contentious hardfork.

2. Bitcoin works perfectly with hardforks.

Satoshi Nakamoto's whitepaper establishes a conflict resolution mechanism that works. But it is not desirable. Damages the adoption. This resource should be used only as a last resort and when there is no other alternative.

3. It implies coercion, with non-voluntary impositions.

For a miner's incentive to be effective, it is not enough to be the first to publish the next valid block. It is also necessary that the owners of most of the *hashpower* decide voluntarily to work to continue with exactly that block.

It is a consensus, without coercion, totally legitimate.

4. It won't work better than the market.

No one is better than miners at making decisions about their own businesses.

5. It is not possible to represent 100% of the hashpower.

True, but it's easy to represent most of the *hashpower*.

Dividing the total *hashpower* into only 100 participants, 97.9% of the SHA256 *hashpower* (Annex III) could be represented with 16 *pools*, including 6 participants corresponding to unknown *hashpower*.

This technical-operational limitation can be mitigated by increasing the consensus needed to make decisions beyond 51%.

6. BMP is vulnerable.

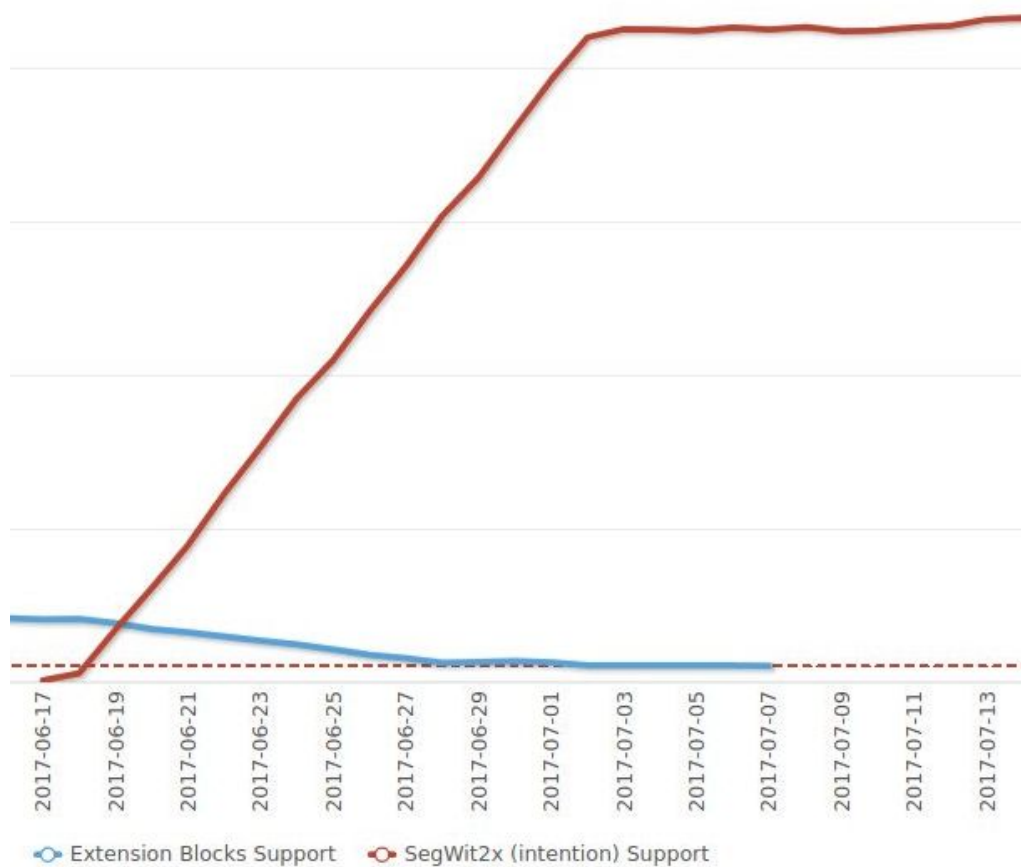
The origin of the legitimacy of the BMP is the *blockchain*. All or part of the operational information can be stored on-chain. It cannot affect the normal functioning of Bitcoin.

Annex II

Informally, the Bitcoin miners already exist as an entity.

On June 19, 2017, 85% of the *hashpower* signaled */NYA/* on the *blockchain* in a stable manner for 5 months. This event took place practically in unison, showing a previous coordination around a target date.

Uncoordination doesn't make straight lines.



Source: coin.dance

Annex 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

Annex IV

Miners, as an entity, can talk.

In the same way that they choose by consensus the next block of the *blockchain*, with the appropriate system, the miners will be able to propose messages and decide by voting which is the next message, in the context of a conversation.

The conversation can be between the entity and an individual, but also between the entity and itself, responding to its own messages, deliberating and establishing in the process its own unified and representative opinion -with the *hashpower* as conductor- of the collective intelligence of the miners, in the context of a meeting.

Annex V

Example mockups.

Home Voting Ended Vote More information Verification

Lorem ipsum dolor sit amet, consectetur adipiscing elit?

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vestibulum aliquet elit metus, sit amet placerat leo gravida eget. Sed dictum leo at mauris varius molestie. Donec accumsan leo in arcu aliquam malesuada.

Result

Legitimacy: **1,577 EH/s OK 81%**

Scrutiny	Hashpower
Yes	1,260 EH/s 76.92%
No	317 EH/s 23.08%
Unknow	245 EH/s

Arguments

+1.7 EH/s Lorem ipsum dolor sit amet, consectetur adipiscing elit. 2 días

```
Bitcoin Mining Parliament - Collective Conversation 178 EH/s 95% hashpower, 197 miners
```

	+ On-chain, according to the project's foundational white paper.	154 EH/s 85%
	+ Off-chain, because the white paper doesn't work.	12 EH/s 6%
	+ Whatever the developers want.	6 EH/s 3%
	+ Let us wait for the markets to solve the problem one day.	2 EH/s 1%

```
14:10 Bitcoin Cash scaling meeting begins. 164 EH/s 88%
```

```
14:13 What is the best strategy for scaling at planetary level? 147 EH/s 84%
```

Next message...

Javier González González - 2018