

Miners are the executive power of Bitcoin

Bitcoin miners are subject to the swings of the market price. This much is true, but it is also true that -if they decide to- they can ignore the short term benefit. This capacity makes them the custodians of Bitcoin's monetary properties.

Therefore, miners have the executive power in the Blockchain.

Miners can write -in proportion to their computing power- in the Blockchain of a network based on proof-of-work. Also -with sufficient consensus- they can write legitimate empty blocks in a minority chain in order to provoke its collapse. And they can do this if they consider this extreme decision convenient to the network and therefore their long-term interests.

Miners can exert their power in real time, in an agile and eminently executive way, recording their decisions in a publicly verifiable way, thanks to the safest and most reliable voting system available which is known.

Therefore, miners are in command in Bitcoin. And they will never act alone, because they form a group of allies without conflict of interest (except in the competition for computing power).

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.

In this Parliament, agreements will be reached, plans will be drawn up to resolve future conflicts, legitimate spokespersons or presidents will be appointed and the selection of the best Blockchain technologies already tried and tested in the altcoins quarry will be speeded up. Furthermore, they will have a closer and more accurate contact with the Bitcoin's community of users and developers.

Satoshi deliberately invented the role of the miners because Bitcoin's future needs to be entrusted to an entity higher than a single person or a small group of developers.

Their existence has been thought to fulfill a purpose and to remain over time. They are the necessary counterweight for the Blockchain to persist over time.

Their legitimate reward are the fees for all past, present and future transactions.

Their interest will be always the same, and therefore their behavior will follow a pattern which is predictable and stable over time.

This is the manifestation of what is known as the Nakamoto Consensus.

Ignoring these facts will give rise to a brittle Blockchain with a tendency to break with every controversy. Accepting the consensus mechanism means the empowering of the miners in order to wield their legitimate power over the Blockchain to its exact degree.

Likewise, accepting this reality could guarantee indefinitely the compliance with the last line of the last page from the Satoshi Nakamoto's original paper, which states:

“Any needed rules and incentives can be enforced with this consensus mechanism.”

Javier González González

GONZO@virtualpol.com

[@JavierGonzalez](#)

1AAtd721LQekC6ncHbAp4ScKxSwR7fFeYT (BCH)

2017-10-31

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

Reference

1. Satoshi Nakamoto, 2008-10-31.
[“Bitcoin: A Peer-to-Peer Electronic Cash System”](#)

Annex I

Map with the keys to the 2017 conflict:

	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?	Lightning 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

Annex II

Hypothetical scenario of the short-term situation.

Soon, the NYA (New York Agreement) will expire and miners will have three options:

- 1) To do nothing and leave the decisions to a vertical and authoritarian team of developers who like takeovers and censorship, and who are unable to develop on-chain solutions because they are focused on taking possession of the future fees that are legitimately due to the miners. The very fact that these fees legitimately belong to the miners is the only long-term incentive to pay for the security of the entire Bitcoin project.
Instead of taking on Satoshi's original architecture, the rate of transactions per second has been artificially strangled and this has caused a setback in Bitcoin's acceptance, which is the basis of Bitcoin's value. And this has been done purely to leave no other option but their private solution of blackmail.
- 2) To make a third hard fork that once again subdivides the community into a third part, to develop new customers, to deploy hundreds of nodes (which would need further expansion), to start the campaign from scratch and all of this just to postpone the conflict.
- 3) To move the hashpower to Bitcoin Cash and assert the Nakamoto Consensus, thereby making Bitcoin Cash -apart from fast and cheap- also the safest option, with more proof-of-work, and therefore worthy of being called Bitcoin. In the same way, the possibility should be considered, if necessary, of mining empty blocks in the minority Blockchain in order to reduce risks and make it clear who is in control.

Annex III

Predictable characteristics of miners as an entity (not applicable at an individual level):

Prudent

Miners have a significant and permanent investment in hardware that only works to mine Bitcoin.

Their prudence is on an unprecedented level.

They will always think long-term. They will measure the risks of each decision better than anyone else. They will prefer deeds to words. They will never act in an improvised or hasty way.

Competent

They are the survivors of a technological career so competitive that it could break Moore's Law. Their technical level can only be up to date.

Keepers of their word

No one wants to reach agreements with those who renege on their word, so the miners will keep their promises. They will not make commitments that they cannot fulfill with certainty.

They have fulfilled their part of the NYA and the Blockchain itself is the best proof of their reliability.

They are able to wait until the NYA agreement expires in November -in spite of the fact that this damages Bitcoin's acceptance- just so that no one can accuse them of breaking their word.

Diplomatic

They only win together. Therefore they will always seek consensus. They have reached out to Segwit2X as a trade-off peace, despite ceding power and only postponing the problem.

This has been an act of generosity in exchange for a certain stability that they can appreciate better than anyone.

Precise

An error on the Blockchain could be fatal.

An error of understanding or strategy would leave them out of the picture.

Even a non-lethal wrong move is unacceptable to the miners.

Capable

They are able to keep the necessary infrastructure with a growing budget.

And to develop software even with several teams.

They will be able to keep enough nodes of any size with the help of Moore's Law.

Reliable

They are interested in their own benefit, but their own benefit is inherently aligned with Bitcoin's well-being and future continuity. This is how it was programmed by Satoshi and we all agree on that common goal.

Annex IV

Counterarguments to the most frequent objections:

1. Satoshi set the limit of 1MB.

He did this as a temporary security countermeasure, when the average per block was a few kilobytes and they were not filled. Unacceptably, some people have seen this as their opportunity to legitimize the strangulation of the network's capacity.

2. Bitcoin's original design does not scale.

The current Blockchain has a size of 140 GB. There are servers with 36 bays of 3.5" and 12TB disks. In this way, we can store 430 TB in a single machine, being able at the present to store the Blockchain 3,071 times. Moore's Law is a mere observation, but it is working. And it says that the capacity doubles every two years. Thus, it is estimated that in 2020 each supernode will be able to store 6,034 times the current Blockchain and in 2030 about 193,088 times (27 BP). Moore's Law can be also applied to bandwidth, latency, disk readings and computing power. In addition, while not yet necessary, there are other options such as mainframes (large unconventional computers), distributed systems (clusters) and cloud computing.

And all this without considering that those developers focused on on-chain solutions will probably find optimizations and strategies to scale up, if and when needed.

3. Mining is a monopoly of a single company.

There are two GPU manufacturers and a few more CPU manufacturers. Distribution is proportionate to the size of each market. All that is needed to practice mining is in the public domain and there is no barrier to free competition. It is foreseeable that the number of competitive ASIC chip manufacturers will increase over time.

4. Segwit already means an increase in the block limit.

This is true, but the increase in practice is insignificant.

5. Bitcoin Cash is an altcoin.

Bitcoin Cash respects the original design. Bitcoin Core decided at some point to substantially modify the original design. Henceforth, it must always be done in an altcoin.

6. Miners need the nodes to accept their Blockchain.

The development and deployment of non-mining nodes is cheap and affordable for miners. The nodes only confirm, they never reject transactions, because they could be ignored. Therefore, the nodes have no power at all.

7. Bitcoin Core's development team is meritocratic.

IRC networks, forums, blogs and social networks are structured in a vertical hierarchy. They are the purest form of authoritarianism, where the founder -the first to arrive- alone has absolute and irrevocable power. This primitive system of decision-making -in the event of a controversy- tends to degenerate into despotism, censorship and the expulsion of discordant participants, which is the antithesis of the miners' behavior.

This damages diversity, creates caves of opinion and fractures the community.

The solution is for several teams of developers to compete with each other.

8. Bitcoin is more democratic or decentralized with small nodes.

Bitcoin is not democratic (without idealizations). Double spending is forbidden, but not double voting. Furthermore, this scheme would be based on IP addresses, which are very cheap. Non-mining nodes have no power over the Blockchain and so their number, size and location is irrelevant.

9. Developers can switch to an algorithm that is resistant to ASIC chips.

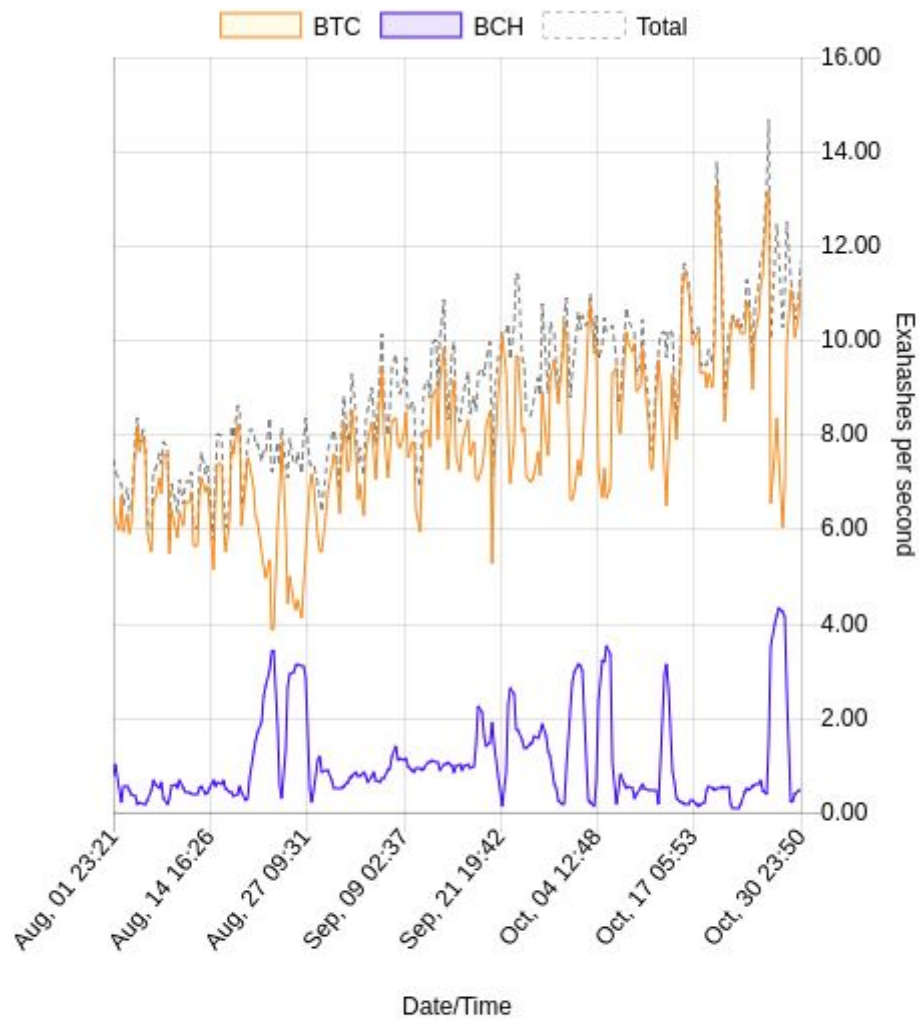
They can do it, but that wouldn't be Bitcoin. It is very risky and involves a new hard fork. It is only a matter of time before someone makes specific chips for any algorithm, which would involve successive arbitrary changes probably decided on by a vertical and authoritarian team of developers against their own mining community.

Therefore, changing some miners for others does not solve anything because it means returning cyclically to mining empowerment.

Annex V

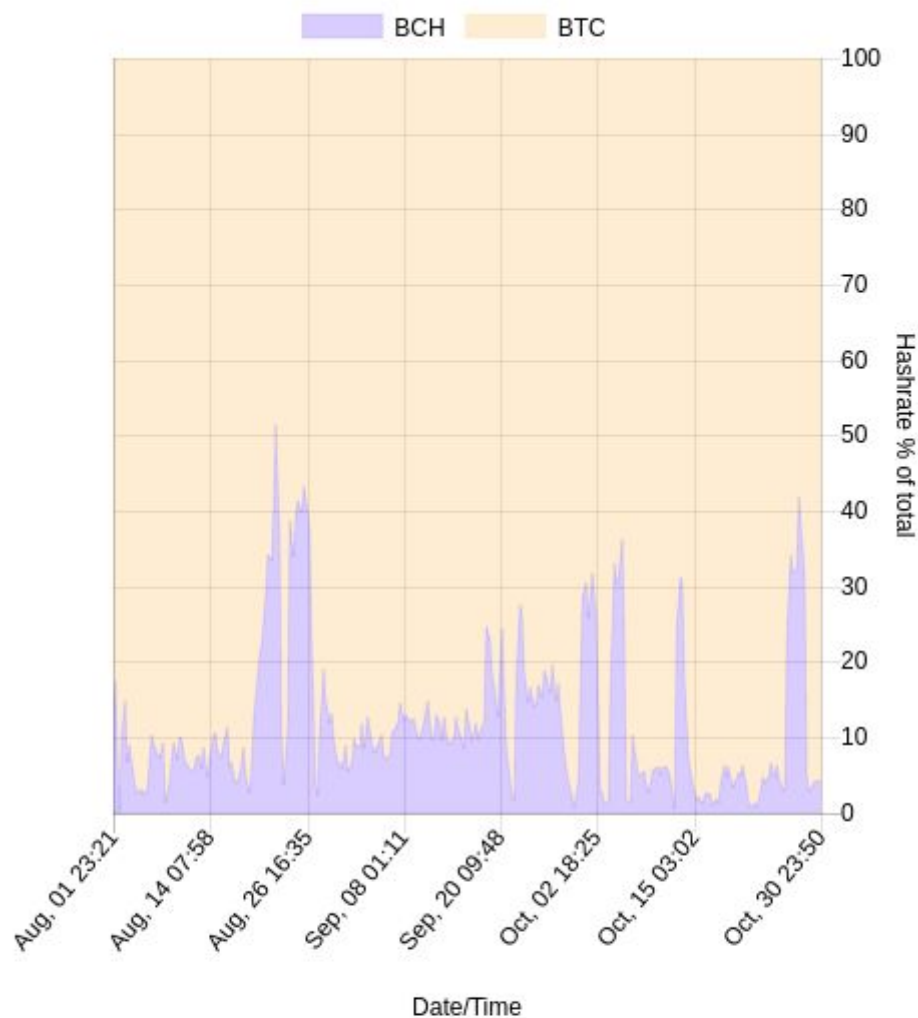
Related facts:

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

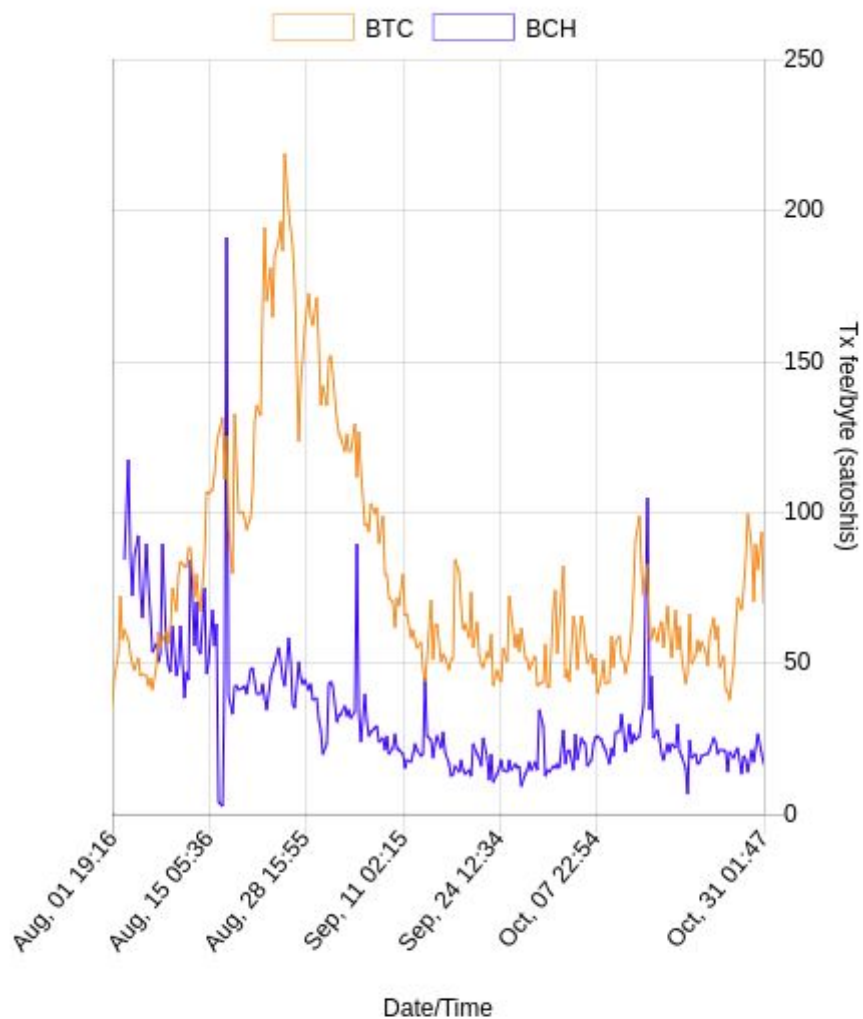
Relative hashrate in percentage of total (stacked, 3h averages).



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

Source: fork.lol

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
------------	-------------------

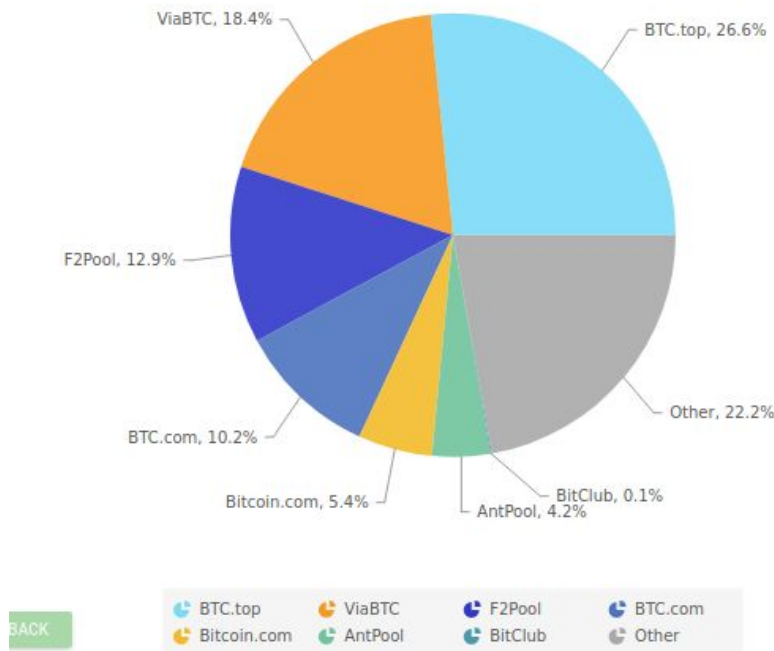
Hash Rate	10,472,053,287 GH/s
-----------	---------------------

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

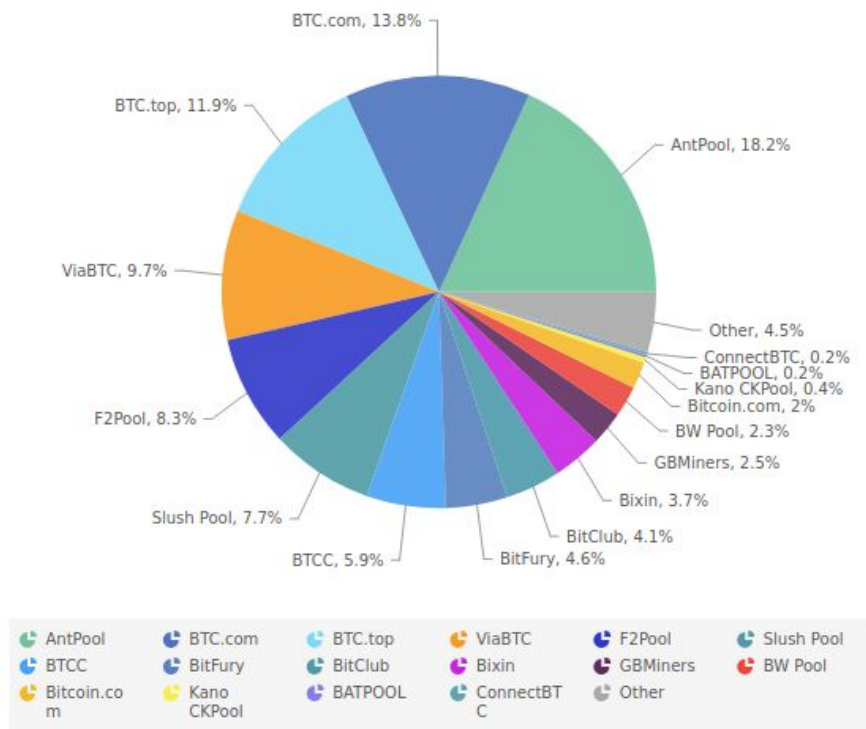
MARKET SHARE			
TOTAL: \$182,517,287,992			
CURRENCY	PRICE	MARKET CAP	MARKET SHARE
BITCOIN 	\$6393.34	<u>\$106,490,744,430</u>	<u>58.35%</u>
ETHEREUM 	\$307.70	<u>\$29,367,013,714</u>	<u>16.09%</u>
RIPPLE 	\$0.20	\$7,784,989,187	<u>4.27%</u>
BITCOIN CASH 	\$449.97	\$7,537,577,081	4.13%
LITECOIN 	\$56.36	\$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%

Source: 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




Source: coin.dance

Annex VI

Open letter I wrote on March 25, 2017 published in *Bitcointalk* and *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,

Sources: [reddit.com/r/Bitcoin](https://www.reddit.com/r/Bitcoin) y bitcointalk.org (archive.org)