

矿工是比特币的行政权力所在

比特币矿工被市场价格的浮动所支配。这一点属实，但同样属实的一点是——只要他们想——他们可以忽略短期利益。这种能力让他们成为了比特币货币财产的卫士。因此，矿工们拥有区块链中的行政权力。

矿工们可以根据他们的挖矿算力在区块链内根据工作量证明记账。同时，如果达成足够的共识，他们也能在少数链中记入空白区块，以导致其解体。如果矿工们认为这样极端的决定能够为比特币网络以及他们长远的利益服务，他们就可以这么做。

矿工们可以实时使用他们的权力，以一种敏捷且有高度行政权力的方式，记录下他们的决策并且能被公开验证，这得益于我们所知的最安全、可靠的投票系统。

因此，矿工们控制着比特币。并且他们永远不会单独行动，因为他们组成了一个没有任何利益冲突的联盟（在算力上的竞争除外）。

作为一种新型的行政权力，很有可能在不久的将来，一个虚拟且透明的比特币矿业议会（BMP）将会成立。在那里，每一个成员可以根据自身所占每秒全网算力比例，发表言论和投票。

在这个议会中，为了解决未来的争端，协议将被达成，计划将被制定，正式的发言人或主席将会被任命，并且在竞争币上充分尝试和测试过的对最佳区块链技术的选择将会被提速。此外，人们能与比特币团体中的用户和开发人员建立更亲密和准确的联系。

中本聪有意发明了矿工这个角色，因为比特币的未来需要交付给一个高于个人和一小批开发者的团体。他们的存在已经被认为是为了实现一种目的以及长远地存在。他们是保持区块链的长期平衡的必要条件。

他们合法的奖励便是所有过去，现在和未来的交易的费用。

他们的利益将永远保持一致，因此他们的行为将会遵循长期稳定且可预见的规律。

这是被称为中本聪共识的声明。

忽略这些事实，将会造成一个脆弱的区块链，每一次争议都让其有瓦解的倾向。接受这种共识机制就意味着赋予矿工权力，以此向区块链精准地行使他们的合法权力。

同样地，接受这一现实，可以无限期地保证与中本聪原始论文中最后一页最后一行言论的符合，如下：

“任何必要的规则和激励政策，可在这一共识机制下执行。”

Javier González González

GONZO@virtualpol.com

[@JavierGonzalez](#)

1AAtd721LQekC6ncHbAp4ScKxSwR7fFeYT (BCH)

2017-10-31

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

参考文献

1. 中本聪, 2008年10月31日。
[《比特币：一种点对点的现金支付系统》](#)

附录 I

带有注解的2017争端地图：

	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 frecueny?
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

附录 II

短期内事态的一种假设情况。

很快，NYA（纽约协议）将失效，而矿工们将面临三种选择：

- 1) 不作为，把决定权交给以热衷于权力接管和审查制度的开发者组成的垂直化且专制的团队，并且这一团队并没有能力开发出链上解决方案，因为他们太专注于掠夺本该合法归于矿工们的未来的费用。正是这些费用理应由矿工们获得，是唯一保持整个比特币项目稳定的激励因素。
与发展中本聪最初的构建背道而驰，每秒交易量被人为地压制，这也使得比特币的接受度遭受挫折，而接受度是比特币价值的基础。而这么做的唯一目的，就是让人别无选择，只能选择勒索式的私人解决方案。
- 2) 生成第三个硬分叉再一次地把社区分割到第三块，开发新的顾客，成百上千个节点（这就会需要更大的扩展），从头开始做宣传活动，而这所有的一切都是为了延后争端。
- 3) 把算力转移到Bitcoin Cash上，并且主张中本聪共识，因此让Bitcoin Cash成为既是快速廉价，又是最安全的选择，随着更多的工作量证明，将会配得上被称为比特币。同样地，如果必要的话也应该考虑这一可能性，通过在少数链上打包空块，以降低风险，也是一种对拥有控制权的展示。

附录 III

矿工们作为团体以后，可预见的特点（不适用于个人级别的矿工）：

谨慎

矿工们拥有重要且永久的投资，那就是只能用于开矿比特币的硬件。

他们的谨慎行事将处于空前的水平。

他们会总是考虑长远情况。他们会比任何人都能预估每一个决策的风险。他们会视行为重于文字。他们永远不会即兴或是着急地行事。

能力强

他们是科技职业道路上的幸存者，这一竞争是如此激烈，甚至可以打破摩尔定律。他们的技术水平必须是最前沿的。

守信用

没有人会想和出尔反尔的人达成协议，所以矿工们将会非常守信。他们不会作出自己不能确信可以完成的承诺。

他们已经做到了自己在NYA（纽约协议）中对应的职责，区块链本身就是他们可靠性的最好证明。

他们可以等到NYA协议在十一月的失效——尽管这会损害比特币的接受度——但这样没有人可以说他们不守信用。

善于外交

他们只有团结在一起才能胜利。因此他们总是会寻求共识。他们达成了Segwit2X这一折衷的和平，尽管需要割让权力，并且这也只是在延后问题的发生。

这是一种慷慨的举措，用来交换稳定性，而稳定性也是他们最看重的。

精准

区块链中的一个错误就可能是致命的。

而理解或战略中的一个错误就可能让他们被淘汰。

哪怕是一个非致命的错误，对矿工们来说也是不可接受的。

能干

他们能够以增长的预算来维护必要的基础设施。

用几个团队来开发软件。

他们将能够在摩尔定律的帮助下保持任何体系的足够节点。

可靠

他们在乎自己的利益，但他们的利益是内在地与比特币的利益和未来的延续性一脉相承的。这就是中本聪当时计划的方式，并且我们都对这个相同的目标一致同意。

附录 IV

对目前一些反对声音的反驳：

1. 中本聪把限制设在1MB。

他这么做是作为一种临时的安全对策，当时每个区块的平均值只有几个KB而且并没有被填满。不可接受的是，有人把这作为他们遏制网络承受力的正当理由。

2. 比特币最初的设计无法升级。

目前的区块链大小为140GB。有些服务器有36个3.5寸的驱动器槽和12TB的硬盘。这样说，我们可以在一个机器里储存430TB，就可以存储当前的区块链3,071次。摩尔定律仅仅是一个观察，但确实是有效的。定律中说明每两年性能提高一倍。但是，人们估计在2020年，超级节点将能够储存目前区块链的6,034倍，而在2030年将会达到193,088倍（27PB）。摩尔定律也适用于带宽、延迟、硬盘读取速度和算力。此外，虽然并不是必须的，也还有其他的选择，例如主机（大型非传统电脑），分布式系统（集群）以及云计算。而这一切都还没有考虑，这些侧重于链上解决方案的开发者们很有可能会找到优化方案和战略来进一步扩容，一旦有必要的话，在必要的时刻。

3. 开矿就是单个公司的垄断。

世上有两个GPU生产商和好几个CPU生产商。根据每个市场的大小来进行分销。开矿所需的一切属于公开的领域，没有任何对自由竞争的阻碍。可以预见的是，互相竞争的ASIC芯片生产商数量将会在未来增多。

4. Segwit 已然意味着区块上限的增加。

这属实，但是这种增加在实际应用中是微不足道的。

5. Bitcoin Cash是一种竞争币。

Bitcoin Cash尊重原始的设计。Bitcoin Core在某个时间点上决定整体修改原始的设计。从那以后，这必须通过一种竞争币来实现。

6. 矿工们需要节点来接受他们的区块链。

非挖矿节点的开发和部署对矿工们来说是廉价且承担得起的。节点仅仅是确认交易，从来不拒绝交易，因为它们可以被忽略。因此，节点并没有任何权力。

7. Bitcoin Core的开发团队是精英领导的。

IRC网络、论坛、博客和社交媒体构建于垂直化的等级制度之上。这些是专制主义最纯正的形式，在这些地方创始人——最先来的人——有最绝对和不可否决的权力。这种原始的决策系统在争议发生之时，就会倾向于恶化为专制、审查制度以及开除持有反对意见的参与者，而这是与矿工们的行为背道而驰的。

这将会损害多样性，创造出驱逐异己的意见洞穴，和社区的裂缝。

解决方案是让许多个开发者团队互相竞争。

8. *比特币在小节点的情况下更加民主或去中心化。*

比特币并不是民主的（去掉理想化以后）。双花是禁止的，但双重投票则不是。此外，这一论调是基于IP地址的，而IP地址是很廉价的。非开矿节点对区块链没有任何权力，所以它们的数量、体量和位置都是无关紧要的。

9. *开发者们可以切换到一种可以抵抗ASIC芯片的算法。*

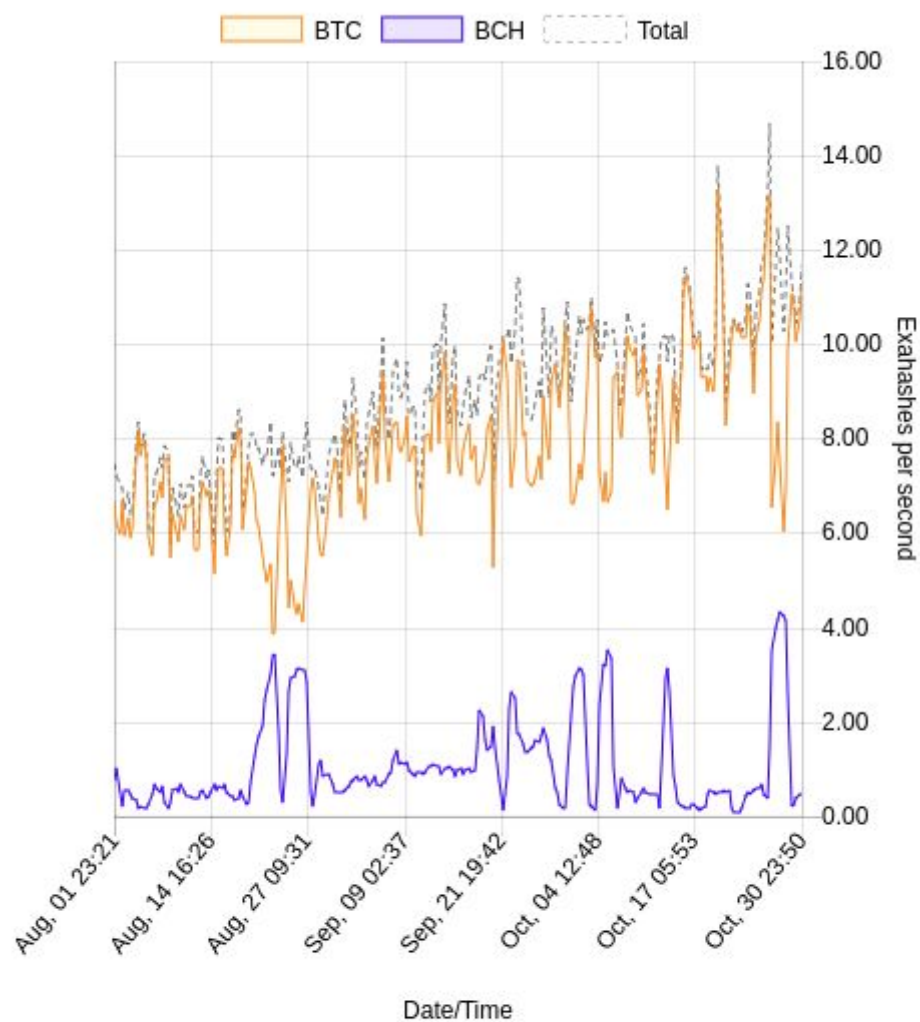
他们可以做到，但那就不会是比特币了。这风险很大，而且还会牵扯到一个新的硬分叉。任何人要针对某种算法而做出芯片，只是时间问题，会涉及一连串的武断的改变，很有可能是由一个垂直化又专制的开发者团队决定的，与他们自己的挖矿社区对抗。

因此，替换一些矿工并不解决任何事情，因为这意味着周期性地反复赋予挖矿以权力。

附录 V

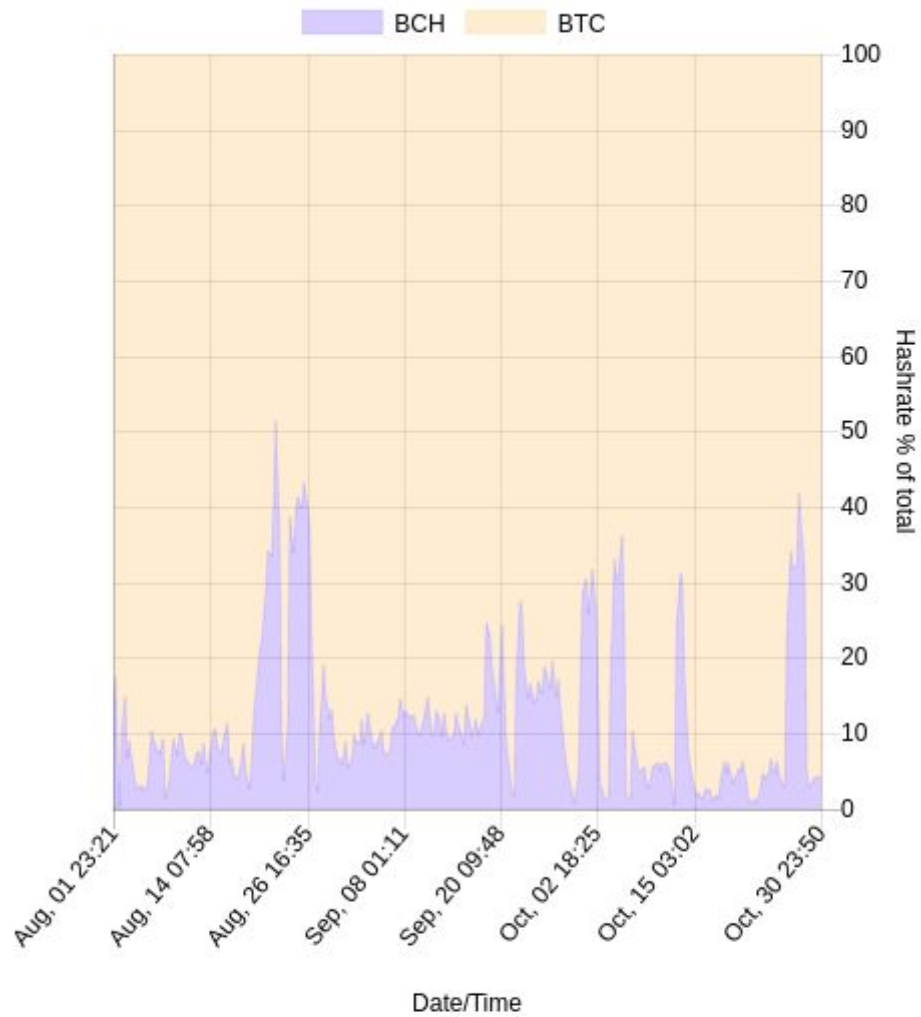
相关事实：

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

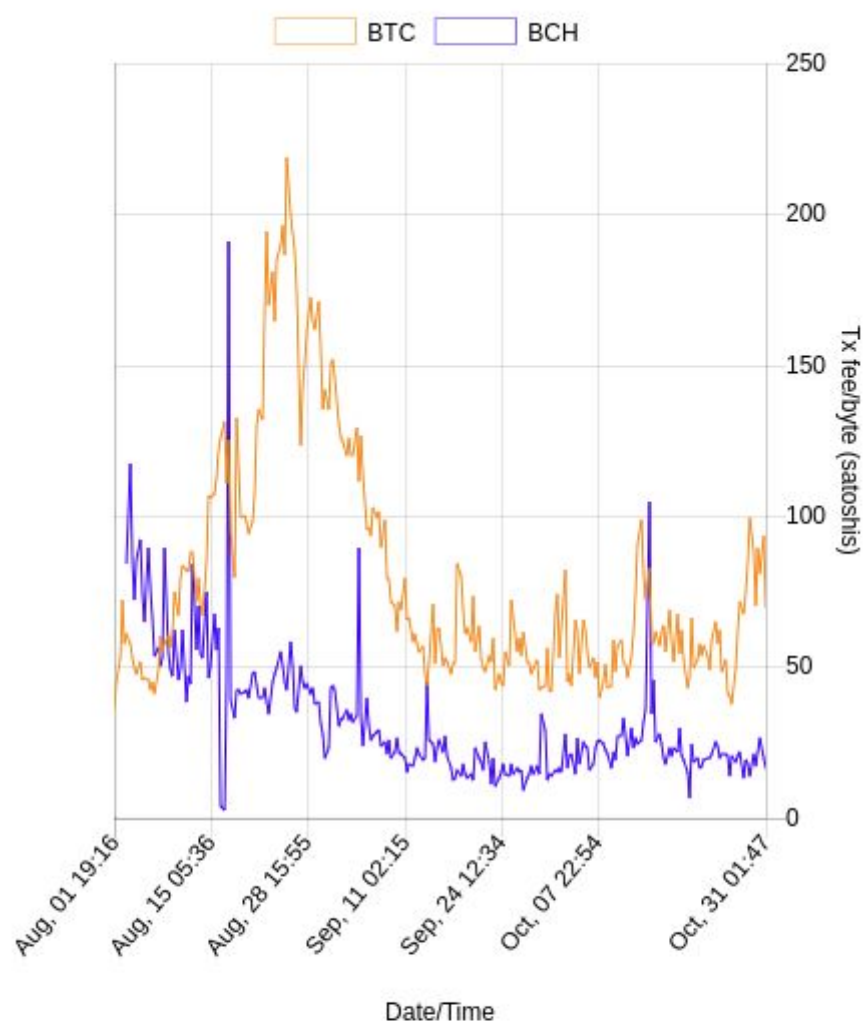
Relative hashrate in percentage of total (stacked, 3h averages).



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

来源: 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
------------	-------------------

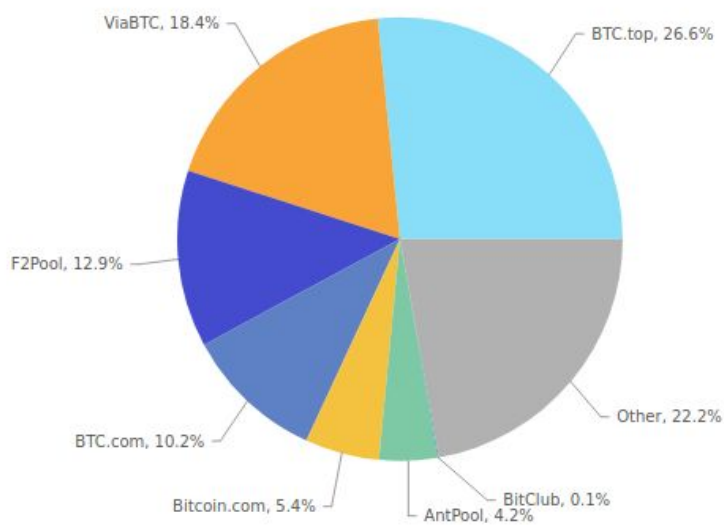
Hash Rate	10,472,053,287 GH/s
-----------	---------------------

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>	58.35%
ETHEREUM 	\$307.70	<u>\$29,367,013,714</u>	16.09%
RIPPLE 	\$0.20	\$7,784,989,187	4.27%
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%

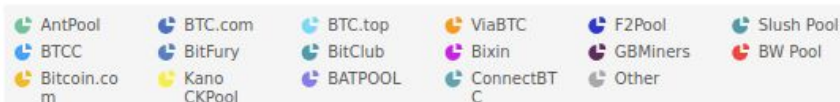
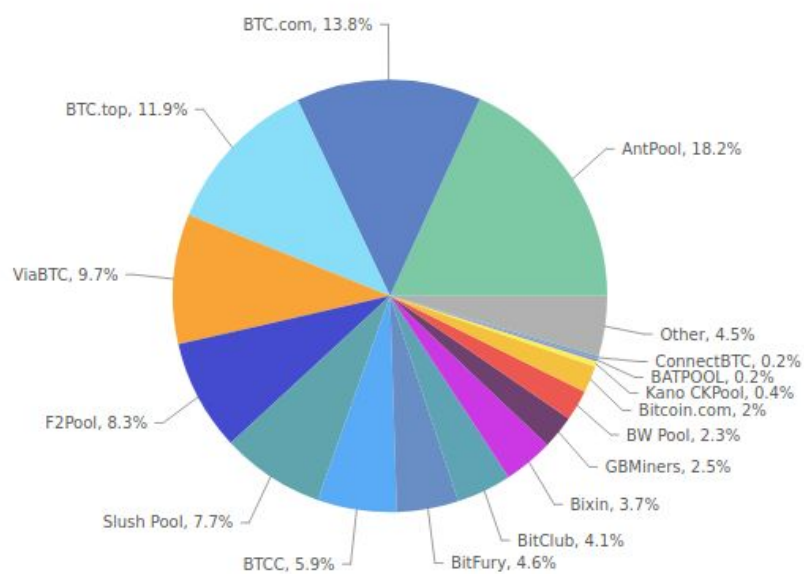
来源: flipping.watch

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



BACK

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




来源: coin.dance

附录 VI

我在2017年3月25日发布在*Bitcointalk*和*Reddit*上的公开信：

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,

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