# 比特币矿业议会

***精华摘录.*** *作为一种新型的行政权力，很有可能在不远的未来，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。*

*矿工是比特币的行政权力所在 2017-10-31*

目前，比特币矿工们就相互协调不足的问题达成共识。

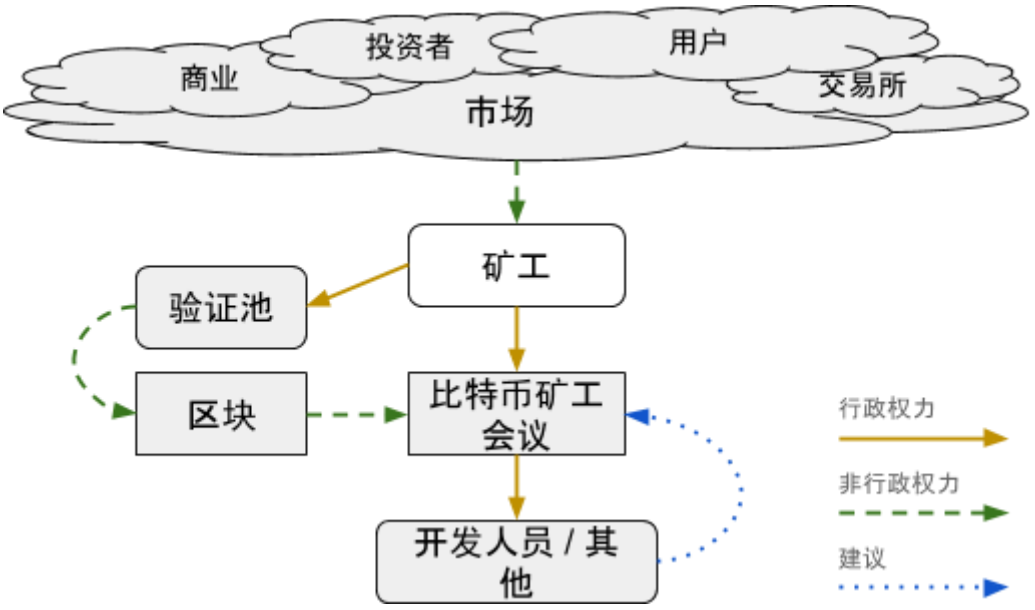
这会导致有争议的硬分岔（hardfork）分割区块链，破坏区块链社区，造成混淆和产生损害。而矿工们则可以比其他人更好地承担责任，防止再次发生此类事件的风险。

在技术发展过程中，在同一区块链中常常出现两个有效但不兼容的解决方案。因此，区块链技术的发展需要有人进行决策。

人们陷入冲突的倾向是一种可以预测的模式。随着多个区块链技术开发团队的竞争，冲突的产生只是时间问题。为了解决这个问题，矿工必须承担起他们刻不容缓的角色。

而且，在技术竞赛中，加速度矢量（acceleration vector）是造成差异的决定性因素。这样，区块链能够以更快的速度在技术上发展，从而在全世界范围内征服更多人，让更多人采纳。

为了成功实现全球对比特币的采用，比特币矿工必须进行有效协调。



通过对算力（hashpower）的投票，比特币矿工可以作为一个实体而行动。

协调好的矿工们可以像一个虚拟的拜占庭式将军一样，形成一个被认作是比特币矿工声音的合理共识。这样，矿工们的决定所产生的影响，无论好坏，都将完全落在他们身上。

合法性是比特币矿业议会（BMP）具有约束力的先决条件。合法性将通过明确的可验证性来实现，该验证将直接从区块链块发出。

这些验证池（pools）只是算力（由那些决定和他们一起挖矿的人所贡献的）的临时代表。该类验证池可以在无风险和易操作的情况下更换。因此，这些验证池没有行政权力。矿工则拥有行政权力，因为是他们在控制采矿机械和融资。

在每个区块币基（coinbase）的交易中，矿池必须公布多个输出中的主要矿工的地址，在OP_RETURN指示中对应于每个矿工所对应算力的百分比。

```
Description         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%)
```

每个矿工的个人算力是用他在区块链中所注册的配额来计算的。一个矿池将永远无法控制比在它区块中所展示的算力更大的算力。

通过这种（超越区块链以及与矿工算力成正比的）方式，每个矿工都能证明他的努力。

信号化（signalization）的实施取决于矿工的意愿。这一愿景可以通过将算力转移到在每个区块中发布该信息的验证池来表达。

当大多数算力参与时，比特币议会（BMP）将会具有约束力。
比特币矿业议会可以以多种形式实施。

我将介绍我的观点和经验中最成熟的一部分：

- 无需更改区块链协议或挖掘方法。
- 该空间必须是虚拟的 （通过互联网） 以表示算力的最大可能百分比。
- 在理想情况下，数据库可以存放在链上，但在一些情况下，它必须在Web服务器上运行。这里的根本要求是，合法性必须牢牢扎根于区块链，因此，合法性是可以普遍验证的。
- 透明度将有助于用户社区对决定的理解和查证。
- 基本系统由用户注册组成，他们可以声称与一个或多个比特币地址相关联的算力配额。他们将通过提供签名来证明对每个地址的控制权。通过使用正确的技术，并公开这些信息，比特币矿工将能够证明他们所控制的算力的数量超越了区块链。
- 每个矿工的算力将被显示出来，以表明每秒的算力数量以及相应于其（在区块链中注册总算力量的）算力的的百分比（参见附录5）。
- 通过典型的互联网传播媒介（比如上网聊天、网络论坛、网上信息等），在同一个空间中，矿工们将能够辩论、审议并最终制定投票建议，以获取信息或做出有约束力的决定。

通过这种方式，矿工将能够根据他们算力的百分比投票。在投票结果公布之后，得票最多的选项将合法代表比特币矿工，同时这也将尊重中本聪本人的白皮书。

> ***精华摘录.*** *节点通过自己的CPU计算力进行投票，表决他们对有效区块的确认，他们不断延长有效的区块链来表达自己的确认，并拒绝在无效的区块之后延长区块以表示拒绝。本框架包含了一个P2P电子货币系统所需要的全部规则和激励措施*
>
> *比特幣：一種點對點的電子現金系統 2008-10-31*

Javier González González
哈维尔·冈萨雷斯·冈萨雷斯
@JavierGonzalez
15bdKu8Wfiyie3xP4jVxTNo9KThCeQkiZd (BCH)
2018-06-15
ES EN CN

附录1

对最常见的反对意见的反驳：

*一、本提议将是专制政府或国家的开始。*

矿工对计划其他人的生活并不感兴趣。
他们追求自己的个人利益，而这与市场所看重的比特币在未来的利益是一致的。

- 如果矿工的行为表现不当，市场价格将下跌。
- 如果矿池滥用算力，它们将被替换。
- 如果BMP不可验证，它将被替换。
- 如果大多数算力没有以协调的方式行事，那么将会出现另一个引起争论的硬分岔（hardfork）。

*二、比特币完全适用于硬分叉。*

中本聪的白皮书建立了一个有效的冲突解决机制。但这并不可取，并将损害比特币的全球扩展。只有在没有其他选择的情况下，才应使用此资源作为最后手段。

*三、本提议意味着非自愿的强制。*

为了使得对于矿工的激励有效，仅仅发布下一个有效区块是不够的。大部分算力的所有者决定自愿决定继续工作也是必要的激励。
这是一个没有强制的共识，完全合法。

*四、提议不会比市场的运作效果更好。*

在决策自己的生意上，没有人比矿工更好。

*五、提议无法代表100%的算力。*

确实如此，但BMP很容易代表大部分的算力。
将总算力划分为100个参与者，算力SHA256（附件3）的97.9%可以由16个验证池组成，其中6个参与者对应未知的算力。
通过将决策所需的共识增加到51%以上，可以缓解这种技术操作上的局限性。

*六、BMP很脆弱。*

BMP的合法性来源是区块链。全部或部分操作信息可以存储在链上（on-chain）。它不会影响比特币的正常运作。

*七、矿工不是比特币的行政权力。*

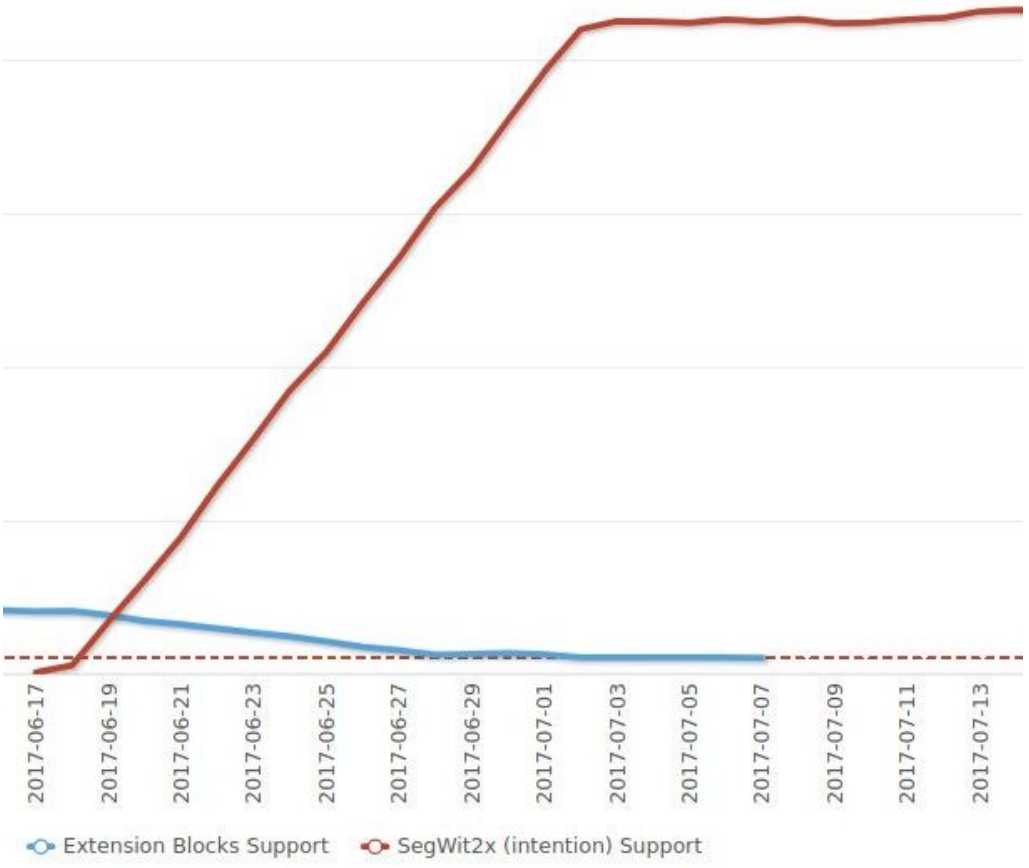
通过非挖掘节点的用户没有权力。
用户通过市场拥有很大的权力。市场是中长期最大的力量，将胜过其他所有国家。但它不是执行官。 它不行动，但会间接地产生反应。
开发者提出共识规则，但最终决定是通过算力来实施的。
矿工们很有竞争力，他们有着全面性的激励，完全控制着区块链，并拥有最安全的投票系统。
因此，矿工没有绝对的权力，而只拥有行政权力，这意味着责任。

附录2

非正式地，比特币矿工已经作为一个实体存在。

2017年6月19日，85%的算力以稳定的方式在区块链上发出了 5个月稳定的/ NYA /信号。这一事件实际上是同调的，显示了围绕目标日期的先前协调。

不协调不会形成直线。




Fuente: [coin.dance](coin.dance)

附录3

| | 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 |

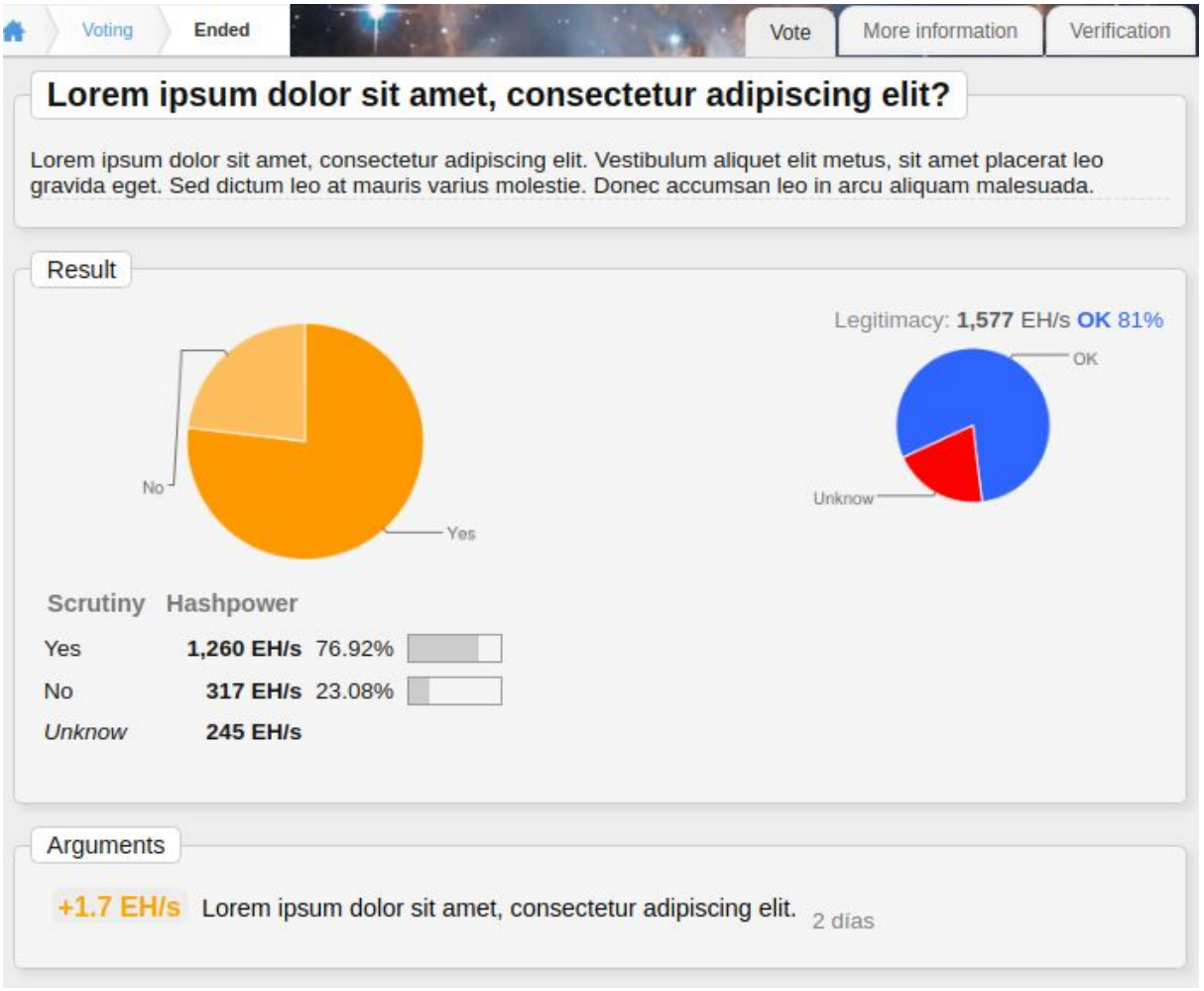
附录4

矿工作为一个实体可以交谈。

在这样一个合适的系统中，与矿工们一致选择区块链的下一个区块一样，他们能在谈话文本中提议信息，并通过投票决定下一个信息。

在比特币议会（BMP）的背景下，谈话可以在其他实体和个人之间（也可以在实体自身之间）对信息作出回应，在矿工的集体智慧下，以算力为指导，在谈判过程中审议并建立自己的统一和具有代表性意见。

附录5
样机.


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
No
Yes
Legitimacy: 1,577 EH/s OK 81%
OK
Unknow
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
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%
+ 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%
Next message...
Javier González González - 2018