

比特币区块容量和未来

今天，BitGo的一个重要客户向我们投诉交易无法确认。为什么不能确认了呢？哦，是因为区块都满了。他们是设置了正确的交易费用的，BitGod平台也每一次都动态计算了交易费用，但是需求激增导致他们的交易一直不得确认。因为比特币内核的缺陷，现在大量的小规模比特币交易所都因此遭受着损失。

所以，我有一些话要说。

#1 比特币开发已经走火入魔

比特币开发员们，我很抱歉，但是你们担心区块扩容就会毁掉比特币这一点是错误的。你们在做的事情，是Donald Knuth告诫你们不要做的——过早优化。一个2MB的区块会不会影响区块传送或中心化，我们并没有确凿的数据。如果你们是正确的，区块扩容确实会需要更多的优化，但我们在碰到真正的问题的时候去优化和解决问题。从我自己构建HTTP/2.0的经验来看，关于优化我只有一点是可以确定的：在你尝试优化之前，你永远不知道有什么可以优化。

过早优化是所有罪恶的根源。Premature optimization is the root of all evil. — [Donald Knuth](#)

#2 我们早有共识

数据显示，90%的社区成员已经同意将区块扩容到至少2MB的大小。如果90%的人的意见不能算是“共识”的话，我不知道什么是共识了。从我在标准制定机构的经验来看，标准永远是需要妥协才能出现的。不论你是否能接受，社区都会按照共识继续前进。

#3 比特币已然中心化

反对区块扩容最核心的观点是，扩容将会导致比特币更中心化。我也希望事实不是如此，但是这场战争胜负已定。从矿池开始，硬件的突飞猛进使个人节点已经如沧海一粟。不管从哪方面考虑，想摧毁比特币如今只需要搞定屈指可数的几家公司就行了。当然，目前比特币还没有像电子黄金（e-gold）那样一家独尊的产品这么中心化，但是它显然已经与中本聪当年设想的去中心化的圣地相距甚远。

请不要误解我的意思，我们都想要去中心化的系统，但是区块容量并不是问题的关键。

#4 隔离见证(SegWit)和闪电网络(Lightning Network)是遥远的梦想

隔离见证和闪电网络都是解决问题的好办法。我都非常喜欢。但是，两者都还没有准备好，也不可能在6到18个月之内开展。闪电网络还更冒风险，有可能最终是完全不可实现的。更进一步来说，如果你认为去中心化对现有的比特币系统而言都是困难的，想想把这个问题再推给一个未经证实的软件是不是更有可能会把问题恶化。不幸的是，我们今天就需要解决区块容量的问题。因为这些还是实验阶段的技术就耽误比特币是一个重大错误。

#5 我们没有时间了

最后一点，我们实在是没有时间耽搁了。一个每天只能处理30万次交易的支付系统是不值得我或者任何人的时间的。我怀疑伊隆·马斯克(Elon Musk)会不会愿意在这么个可怜的微乎其微的系统上花时间。我想拉里·佩奇(Larry Page)，史蒂夫·乔布斯(Steve Jobs)，巴菲特(Warren Buffet)都不会做这样的选择。

如果我们想改变世界，我们就得更有野心。把世界上最大的交易系统乘上1000倍，这才是我们该做的事情。我们没有时间浪费在不能改变世界的系统上。如果你想看到任何改变，现在就可以开始行动了。否则，很快下一代真正的思想领导者就会扔掉比特币，做出真正的创新来改变世界。