每当我声称比特币是唯一去中心化的加密货币时，我总会听到以下两个反击的观点

1.我的X币也是去中心化的。

2.由于比特币的核心开发团队和矿工的存在，比特币并不是去中心化的。

我将在下次回答关于对其他加密货币是否具有去中心化属性以及比特币核心团队的观点，而本篇文章将为你重点解读“挖矿中心化”的观点。

我要回答的问题包括以下几个：

1.比特币挖矿是中心化吗？

2.矿工们如何控制比特币？

3.51%攻击有什么风险？

4.山寨币玩家的观点对吗？

去中心化

去中心化是比特币的一个关键属性。如果移除比特币去中心化这个属性的话，将得不偿失。正是因为有许多中心化货币发行者，才会导致通货膨胀以及货币储蓄的购买力下降。而山寨币玩家则辩称，中性化只不过是一个范畴，甚至认为比特币就是中心化的。

首先，去中心化并不是一个范畴，有单点故障的系统不是去中心化的，否则不存在单点故障。中心化的东西之所以被称为中心化，是因为可能某个单点故障会让整个系统出现问题。而事实不存在像山寨币玩家所说的介于两者之间的情况，山寨币都有一个或多个这样的属性，并且这些属性会产生单点故障：

1.该加密货币的创建者仍然参与该项目；

2.该加密币有一个强制升级所有用户（硬分叉）的开发团队；

3.该加密币有一个指导其发展方向的基金会或组织。

有的加密币币属性较多，正如以太坊有三种，而门罗币只有第二种。这样，你就可以说，某个项目相比其他可以有更多的单点故障。然而，实际上，只要存在一个单

点故障，代币就是中心化的。这样一来，政府完全可以通过这单点故障，用其想要的制定的任何规定来控制这种货币。比如他们可以逮捕创建者，向开发团队征税，或者将基金会或组织国有化。然而权威接管加密币的方法在这里并不是最重要的，它能够接管的事实才是最值得我们关注的，中心化发行的货币有可能更容易被取代。

这里的问题是比特币挖矿是否是单点故障。
政府或其他机构可以通过控制采矿中的个体矿工来控制比特币吗？
关于这一点的推测有很多，这也是本文的主题。
让我们一起来看看接管比特币到底需要什么条件。

持有集中算力的矿工到底能够做什么？

矿工们的工作就是通过工作量证明来维护比特币网络安全。当单个矿工有51%的哈希算力时，就可以进行网络攻击。然而，这和比特币网络控制大不相同。51%算力攻击自然是有限的，因为它只影响到被攻击的账户持有人例如交易所。这与网络强制升级形成了鲜明对比，网络强制升级可以重置整个余额，抬高货币汇率使其升值或改变各种激励措施。是对整个网络的实际控制。这是其发展的真正瓶颈，因为后者的网络规则是由一个单一群体决定的。而51%攻击可能使一些参与者更容易受到影响。两者各不相同。

这种区别至关重要，因为山寨币玩家常常将二者混为一谈。其实它们是不一样的。前者是带有许多执行条件的攻击向量，最后影响到有限的人数；后者硬分叉有加密货币被完全接管的可能性。打个比方，如果把前者看作是军队防御的弱点，而后者则是征服者为任何目的而接管军队。前者仍然要求攻击者在公开场合决一雌雄，而硬分叉升级只是在核心层力推动的情况下完成的。

鉴于此，我们称之为山寨币中心化。它们可能被少数人的一时兴致所接管、征服和改变。然而控制大量的挖矿哈希算力与此不同，而且影响也很有限，更别说执行成本高。这就是单独负责银行账户者之间的区别，其中有些人会贪污，携款潜逃等等。并且一个有效的电汇也有可能不得不等待很长时间之后才被存入。

如何达到51%的挖矿攻击要求？

为了说明这一点，让我们看看如何执行51%的挖矿攻击。为了执行51%的挖矿攻击，首先需要比网络其他部分更多的哈希算力，这就意味着要具备大量的采矿设备，当然这也将花费大笔钱。目前这种挖矿设备的交货期很长，同时正是因为这种设备往往非常有利可图，因此收购最新一代矿机也是非常困难的。使用旧设备不失为攻击者的一种选择，但这种设备即使能够节省资金并且便于操作但却效率低下。无论

是哪种方式，设备本身以及操作设备成本是非常高的，这需要巨大的资本投资，并且还需要与那些公然挖矿并从中赚取丰厚利润的矿工们竞争。

除此之外，攻击者具备挖矿设备还往往不够，还需要大量电力。大多数的比特币挖矿都是以电力供应商的电力盈利能力为代价而完成的。挖矿更倾向于移动到能源聚集地。因此，水力发电大坝、太阳能电池板农场和位于边缘的地热发电往往是挖矿设备的动力来源。一般矿机的电价为0.025美元/千瓦小时至0.06美元/千瓦时不等。这往往绝对是最低的电价，大多数情况下电力公司都要求签署长期合约才能以如此低的价格供电。

在过去几年里，由于价格的上涨，以及由此产生的能源需求愈大化，很难获得足够的电力来经营一个采矿场。当比特币网络规模还很小的时候，也许才有可能获得足够的电力来运行设备，并且能够提供51%哈希算力的设备，但随着时间的推移，这种方法越来越不可行。比特币网络消耗的能量继续增长，攻击者需要获得大量的电力才能成功地实施攻击。

也许有一些电力公司可以同时满足51%的网络能源消耗，但如果想说服他们能够一次就能卖给你这么多的电力，只能祝你好运。在电力行业，消费者往往签订大量长期合同，一两周的短期以及高强度电力供应是不切实际的，即使如此，成本往往会很高。请记住，工厂、企业和农场甚至家家户户都依赖于这些发电厂提供的电力来保持每天的正常运转。所以不能仅仅为假想的攻击者提供电力而不考虑大部分用户的用电情况。

换言之，作为一个攻击者，需要获取大量的电力，如果自己不控制电源的话，电力便难以提供。因此，攻击者不仅要控制51%的潜在哈希算力，而且可能还需要自己发电。

利润驱动的挖矿攻击

51%攻击的资金成本是巨大的。将需要大量的高效挖矿设备和一吨电力，这两者都难以兼具。这也就意味着，你可能需要生产自己的挖矿设备，并能自己发电。这可能需要数年的筹备时间来生产设备以及签署长期合同以获得所需的电力。考虑到经济效益，只有在你能从挖矿攻击中获得足够的收益，从而使风险物有所值的情况下，投资这么多的资本才会有意义。有几种方法可以尝试从51%攻击中获利，包括做空市场或尝试进行双花，但它们都需要通过交易来获得资金并保持正常运行。在过去，这很容易，但由于围绕大多数交易所的反洗钱或者实名认证法律，这种情况已不复存在。

此外，如果真的能按上述方案实施51%攻击的话，就意味着攻击者通过公然挖矿获

得巨大的收入。这样做显然风险低得多，因为你不需要51%的网络算力，这样预先需要的资本投资要少得多，

换句话说，再从经济学的角度上看，由于涉及到的成本和风险之高，进行51%的攻击是没有任何意义的。当然，用这种方法攻击哈希算力低得多的山寨币反而经济得多。

主权攻击

51%的挖矿攻击，其真正潜力来自于国家级的参与者。假设它是一个单一的主权国家，这样的实体根本不需要关心成本，就能够获得巨大的能量并且有攻击比特币的动机。同样，这并没有给予攻击者对网络的控制，攻击者只是具备攻击一小部分网络的能力。撇开动机不谈，让我们看看实际情况。

为了实现这样的目标，即使是一个主权国家也需要协调许多部分的工作，才能使其运转。政府需要通过自己的工厂或通过征用所需的设备来获得大量的哈希算力。不可能长时间秘密进行，并且社会很可能有能力为此做好准备。同样，政府也需要以同样的方式获得大量的电力供应。再次重申，这不可能是一个长时间的秘密行动。政府还可能进行必要的军事层面协调，而大多数政府可能不知道如何协调。

那么这一切都是为了什么？在特定交易所上进行的双花攻击？同样，这样的攻击不会摧毁比特币。比特币网络的其他部分还会继续运行，如果攻击持续下去，也会以分散的方式消除即使是最杂烩重的攻击。这绝不是一个单点故障，因为简言之，比特币不会那么容易地被摧毁。

为什么山寨币玩家对51%的挖矿攻击紧追不舍？

因此，问题就转向为什么这么多的山寨币玩家经常提及比特币51%攻击这个问题。

首先，这是人们认为比特币仅有的脆弱属性之一。 请记住，山寨币是比特币的竞争对手，它就像任何一个竞争对手一样，山寨币吹嘘比特币容易被51%攻击，从而让自己看起来更好。 这样一来能够使人们减少对山寨币具有明显中心化缺点的关注。

其次，他们通常试图出售股权或储备或其他无稽之谈概念。这是他们展示系统优势的方式。大多数山寨币玩家之所以支持他们手中的山寨币，因为他们真的希望他们的是比特币。他们希望手中的币价格暴涨，想要像特雷·迈耶这样的超级富豪投资者一样富有。但这由嫉妒驱动，也是人之常情，我另一篇文章将重点描述这一点。

结论

尝试自己印钱者抑或是新货币领域的精英大多都过分夸大比特币的挖矿攻击。 51%的攻击成本太高并且不经济，产生的收益太少又不能产生更多的钱，而且只会影响到一些公司和个人。

甚至有可能是51%的攻击导致100个比特币或更多比特币的交易中断，这对比特币来说未必是件坏事。就像比特现金硬分叉一样，这样的事件可能会证明比特币的抗脆弱性，并引发大规模的价格反弹。