

比特币矿池是由第三方组织和运营的去中心化团体，以协调来自世界各地矿工的哈希算力，然后根据贡献给矿池的算力按比例分享任何产生的比特币。

为什么要在矿池中开采比特币？

在某种程度上，比特币挖矿（更一般地说，工作量证明挖矿）是“猜测”比特币区块链中的下一个区块可能是什么的过程。

通过将随机数（“nonces”）与（潜在的）比特币区块的所有其他内容相结合，生成的“区块哈希”可能是有效的，但这是一个反复试验的问题。专门的挖矿硬件旨在每秒进行大量猜测，但对于每个单独的猜测，结果不太可能得到验证。

采矿的随机性使个体矿工面临很大的差异或“运气”。即使一个非常大的矿工控制了比特币网络上所有哈希算力的 1%，也不能保证他们会始终如一地在每 100 个区块中找到一个。取而代之的是，他们可能在某一天幸运地找到了三个区块，但在接下来的三天（或更长时间）内运气不佳并找到了零个区块。

联合挖矿是个体矿工结合他们的哈希算力的一种方式，这样他们就可以像一个大矿工一样进行挖矿。个体矿工（在联合挖矿的背景下，也被称为“散列者”）分享联合矿池发现的任何区块的奖励，并根据他们贡献的散列能力份额进行调整。这保证了他们会更频繁地找到区块，从而平滑挖矿奖励的收益。

通过联合挖矿，矿工可以获得相对稳定的收入，而不是零星的巨额发薪日。

比特币矿池如何运作？

矿池有不同的变体，并且不时提出和引入新的方法。

然而，最典型的情况是，矿池运营商会设置一个服务供哈希器连接。通过此连接，矿池运营商将向哈希器发送“块模板”。顾名思义，这些块模板是下一个比特币块的模板，但没有对其执行所需的工作证明（“猜测”）。

使用这个块模板，散列者开始猜测下一个块是什么：他们对其执行工作证明。如果他们猜对了，他们将有效的比特币区块返回给矿池，矿池将区块广播到比特币网络，获得区块奖励。然后它将区块奖励切成小块，根据他们贡献的哈希算力的比例支付给池中的所有哈希（尽管这种操作方法只占比特币网络的一小部分）。

矿池根据哈希率的预期值支付矿工的哈希率。为了赚取收入，矿池通常以折扣价（

预期价值的 97% 到 99%

左右) 购买哈希率。预期哈希率在不同池中的计算方式不同, 但通常遵循 $1 / \text{网络难度} \times \text{区块奖励} + 24 \text{ 小时平均交易费用}$ 的公式。

矿池可以通过查看哈希结果并将其与网络目标进行比较, 立即验证提交给他们的工作是否有效。矿池设置了一个自定义阈值, 称为“共享目标”, 允许矿工大约每五秒向他们提交一次共享(哈希)。如果哈希值低于共享目标, 则它被认为是有效的, 矿工的的努力会得到回报。矿工的哈希率越高, 共享目标就越低, 矿工因“更努力”的工作而获得同等奖励。

这取决于您想要进入的深度级别, 但还有一些细微差别。(1)

你需要一个完整的节点来挖掘 ASIC 不附带的, 因此矿工可以使用 ASIC 挖掘到网络, 而矿池运行完整的节点 (2) 大多数矿工希望获得一致的支出, 无论采矿运气如何所以他们根据哈希率的预期价值直接卖给矿池。大约 95% 的行业以这种方式工作(泥浆池是一个明显的例外)

一些矿池的替代设计不依赖于矿池运营商(相反, 矿池使用一种“迷你区块链”) 或让散列者创建自己的块模板(仍然需要得到矿池的批准)。

矿池中的比特币挖矿更有利可图吗?

平均而言, 不, 在矿池中开采比特币并不比单独开采比特币更有利可图。但是, 从另一种意义上说, 是的。

在足够长的时间线上, 独立挖矿的差异应该会自行解决, 独立矿工的收入至少应该与在矿池中的收入一样多。事实上, 由于矿池运营商通常会为其服务收取费用, 因此单独挖矿可能会更有利可图。

然而, “在足够长的时间线上”可能意味着差异需要比生命周期更长的时间才能自行解决。许多矿工更喜欢更稳定的收入形式, 即使这意味着他们需要支付少量费用。矿池支付一致的奖励而不是基于挖矿“运气”, 这对于具有固定成本(例如电力)的挖矿企业或个体矿工来说极为重要。即使是产生网络哈希率 1% 的矿工也不能冒单独挖矿的收入与成本不匹配的风险。

此外, 挖矿过程还存在很多技术挑战, 例如孤立块和被拒绝的区块、矿工效率低下等。矿池运营商一直在努力完善挖矿流程, 并尽量减少参与者的这些潜在损失。

如何选择比特币矿池

选择比特币矿池对矿工来说可能很困难。有很多选择，而且定价历来非常不透明。矿池可能会向潜在的矿工报价一定的费用，但可能不清楚该费用的依据是什么以及矿工实际会赚多少钱。

选择矿池的最佳建议是尝试多种选择并进行一些自己的测试。这样，您就可以就适合您的游泳池获得更有根据的意见。

除了基准盈利能力外，您还可以根据地理位置（和当地管理法律）、用户体验、性能统计数据 and 可用数据以及随服务提供的其他挖掘工具等因素来选择矿池。

比特币矿池是比特币网络的问题吗？

如上所述，在最常见的比特币矿池设置中，矿池运营商为哈希创建块模板以执行工作量证明。这意味着矿池运营商可以决定在整个矿池正在处理的区块中挖掘哪些交易。这是挖矿中心化的一种形式；在所有其他条件相同的情况下，一个所有比特币矿工都单独开采的生态系统将比他们在矿池中开采的生态系统更加去中心化。

这种集中化为矿池运营商提供了一定的权力。例如，他们可以代表矿池决定不包括某些交易（“审查”），甚至可能尝试执行 51% 攻击（尽管这会更加困难）。

这是否是一个真正的问题，以及这个问题有多大，取决于许多因素。比如看矿池有多大，看算力转矿池的难易程度，或者开新矿池的难易程度。到目前为止，联合挖矿还没有给比特币带来非常严重的问题。

一些比特币支持者对在中国运营的矿池集中表示担忧。由于哈希率的管理如此高度集中在一个国家，因此可能会出现国家支持的攻击。

另一方面，矿池的存在可能首先让更多的人参与比特币挖矿，这也有助于系统的去中心化。（同样，这种去中心化是否真的有用还取决于许多其他因素。）

一些替代的比特币矿池设计（如上所述）试图限制联合挖矿的一些风险，但往往会带来自己的权衡，并且（目前）还没有真正大行其道。由 Braiins 开发的 Stratum V2 是一种创新的矿池集中化解决方案，它允许矿工提交他们自己的自定义区块，从而将一些权力还给他们。但是，尚不清楚其余主要位于中国的矿池是否会采用该技术。

联合挖矿是比特币协议的一部分吗？

不，联合挖矿不是比特币协议本身的一部分，并且没有理由相信中本聪打算通过矿池进行挖矿。

相反，联合挖矿是由 Marek “Slush” Palatinus 在 2011 年发明的，他还创立了比特币的第一个矿池：Slush Pool。矿池使用他们自己的协议，尽管其中一些协议在今天已经变得如此标准化，以至于它们也可以被视为比特币协议的一部分。

当然，虽然它不是为此而设计的，但比特币协议确实允许比特币挖掘。（这就是它可以存在的原因。）

如何在比特币矿池中挖矿？

如果您想在比特币矿池中挖矿，只需将您的挖矿硬件连接到您选择的矿池即可。（如今，没有专门硬件的采矿不再是真正的选择。）它通常就像将矿池的 Stratum 配置放入您的矿工并创建一个工人名称一样简单。矿池的网站应该有更具体的说明如何做到这一点。