PoW vs PoS：攻击的经济成本比较

本文译自 BitMEX Research 的一篇报告，原文链接：https://blog.bitmex.com/pow-vs-pos-economic-cost-to-attack/

摘要：本文对比了攻击 PoW（工作量证明）网络和攻击 PoS（权益证明）网络的经济成本。我们分别分析了租用和购买算力/质押权益的成本。我们纠正了一个普遍的误解，即认为由于需要购买代币，PoS 网络的攻击成本必然更高。我们得出的结论是，理论上攻击这两类网络的成本差异比许多人想象的要小。

概述

本文旨在分析比较攻击 PoW 系统和 PoS 系统最经济的方法，特别是对攻击成本进行最恰当的一对一比较。我们之所以撰写这篇文章，是因为其他人已经做过一些比较，通常得出 PoS 系统更难攻击的结论，但我们认为这些比较并非基于公平的一对一对比。在本文中，我们着重区分租用和购买算力/质押权益这两种方式。我们认为，在比较攻击的经济成本时，需要先确定是考虑租用还是购买，然后再尝试进行一对一比较。

思想实验

让我们先进行一个思想实验。虽然这可能不太现实，但假设 Kamala Harris（卡玛拉·哈里斯）任命 Elizabeth Warren（伊丽莎白·沃伦）为副总统候选人，并且 Kamala Harris 在 2024 年美国总统大选中以压倒性优势获胜。这对加密货币生态来说无疑是一个噩梦。除了作为副总统的常规职责外，我们假设 Elizabeth Warren 还负责加密货币事务。于是，她组建了一支反加密货币部队，拥有数十亿美元的预算，试图关闭加密货币网络。

这个思想实验很有意义，因为加密货币网络的设计初衷就是尽可能难以被关闭。那么，让我们思考 Elizabeth Warren 将如何进行这些昂贵且可能徒劳的攻击，以及它们的成本是多少？接下来我们将对比攻击比特币和攻击以太坊的成本。

全节点和共识规则

许多人认为，与以太坊相比，比特币的一个核心优势在于其拥有大量全节点。这些节点虽然与区块生产无关，但在执行共识规则方面发挥着关键作用。重要的是，这些节点的运行成本很低。许多比特币用户运行这些节点，将它们连接到钱包，并且形成了一种文化：除非整个社区达成了压倒性的共识，否则不会因为共识规则的更改而升级这些客户端。以太坊中不存在这样的情况。

在本文中，我们将尝试暂时忽略比特币的这个明显优势，而专注于攻击 PoW 和 PoS 网络的理论成本。理论上，以太坊也可以培养出与比特币类似的执行共识规则的文化和网络。PoS 本身并不妨碍这一点，只不过运行一个完全验证的以太坊全节点更昂贵，因为需要验证与质押过程相关的签名。在某种程度上，忽略这一弱点，这就是钢铁般的以太坊。

另一个需要解决的问题是，在回应我们下面将概述的一些基本攻击时，以太坊社区的许多人表示，社区会通过共识规则更改来罚没攻击者的质押权益。就本文而言，我们将假设比特币和以太坊都无法有效地做到这一点。另一个考量是，攻击者可能会成功地强制协调和中心化，这是一些人可能想要避免的。也许我们考虑的是未来，届时这两个协议都已经僵化，无法在不造成重大分裂的情况下协调协议的规则变更。

攻击成本

假设比特币价格为 60,000 美元，区块奖励为 3.125 BTC，考虑适度的交易费用，这意味着比特币矿工的年收入约为 100 亿美元。我们认为，这是关键的安全指标，也是最重要的单一安全指标。比特币矿工每年的花费接近 100 亿美元，如果你想攻击比特币，你可能需要与之匹配。但与之匹配到底意味着什么呢？在本文中，我们将在租赁和购买之间进行分析。

租赁

攻击 PoW 网络最便宜的方法是租用算力。理论上，如果矿工的年收入为 100 亿美元，那么只要你给他们的年收入略高于 100 亿美元，具有经济理性的矿工就会愿意把算力租给你。这样的假设也许不太现实，因此，我们假设你需要支付 20% 的溢价来吸引矿工，即每年 120 亿美元。当然，你实际上并不需要每年花费 120 亿美元，因为租到算力后，你每年可以获得 100 亿美元的收入。因此，可以说，租用整个比特币算力的净成本仅为每年 20 亿美元。

现在，如果你是 Elizabeth Warren，你当然只需要 51% 的算力就能发动攻击，让链上充满空区块。另一方面，当成功进行这种攻击时，我们可以假设比特币的价格会急剧下跌。因此，这种攻击的净成本可能是每年 60 亿美元，即以 20% 的溢价租用一半的算力。

同样的逻辑也适用于质押权益。如果以太坊的总质押权益会带来每年 30 亿美元的收入，那么具有经济理性的质押者应该愿意放弃直接质押，以换取每年 30 亿美元的收入。同样，与 PoW 一样，我们也需要假设存在 20% 的溢价，即每年 36 亿美元。这意味着租用所有质押权益的净成本为每年 6 亿美元。或者，如果想要攻击，也许只需要三分之一的质押权益，所以每年仅需 12 亿美元就可以使 PoS 网络完全停止。

因此，我们认为，在考虑攻击的经济成本时，一个关键的可比较指标是比特币每年 50 亿美元对以太坊每年 12 亿美元。如果将市值正常化，攻击成本大致相同，比特币大约是以太坊的三倍。这当然不是一个完美的比较，但在我们看来，在试图进行同类比较时，这已经是最好的对比了。当然，这其中还有许多变动因素，包括比特币挖矿收入的可持续性，与以太坊永久发行形成对比。然而，这不一定是 PoW 与 PoS 的固有特征，理论上，PoW 币也可以有永久发行，或者 PoS 币也可以尝试完全从交易费用中获得质押收入。

至于这种租用算力/质押权益进行攻击的可行性，比特币玩家和以太坊玩家不必过于担心 Elizabeth Warren。这种攻击有些不切实际。事实上，如果攻击开始，资产所有者可以收回他们的算力或质押权益。资产所有者可能会担心，如果网络受到攻击，他们的资产价值可能会下降。当然，在这一点上，以太坊和质押权益似乎更有优势。质押的 ETH 价值 1000 亿美元，超过了比特币挖矿资产的价值。不过，虽然这个 1000 亿美元的数字很重要，但在我们看来，它不是与比特币进行比较的关键指标，年收入更为关键。另一方面，目前排名靠前且已经上市的比特币矿商的市值约为 280 亿美元。这些矿商控制了大约三分之一的比特币算力，因此实际上与 1000 亿美元估值的质押 ETH 确实非常接近。另一方面，这些已经上市的比特币矿商可能会因为 "转向 AI" 的叙事而被高估。同时请记住，比特币的市值是以太坊的三倍多。因此，即使在计算中包含了这些已上市的矿商，以太坊在这一资产价值指标上仍然胜出至少三倍，以百分比计算。以太坊质押者确实有更多的利害关系，这很重要，也许是仅次于年收入的第二重要指标。

上述分析的一个小问题是，非托管算力租赁相对简单。矿工可以在互联网上向承租人提供某种形式的硬件控制权（有限制），然后在攻击发生时取消承租人的访问权。以完全非托管的方式出租你的质押权益并不一定可行，这可能是一个优势，因为这会让质押者更不愿意出租他们的质押权益，因为风险更大。另一方面，这对 PoS 系统来说并不是什么优势，如果矿工出租算力的方式很容易被撤销，那么就不需要担心持续攻击的风险了。当然，非托管质押服务也有很大的好处，人们希望建立这样的服务（以太坊的竞品声称它们已经建立），让质押系统总体上更具弹性，但我们认为，必须始终存在大量的风险，因为罚没风险必须足够大，质押才有意义。

购买和建设

下一种类型的攻击涉及实际购买和建设，包括购买挖矿硬件、设施和电力，或购买质押权益。我们首先考虑购买质押权益。

如果 Elizabeth Warren 的反加密货币部门想要攻击以太坊，她可以尝试购买三分之一的 ETH 质押权益，然后关闭网络。目前，三分之一的 ETH 质押权益价值 330 亿美元。当然，如果有人试图购买这么多的 ETH，尤其是美国政府，那么价格就会暴涨，因此购买的成本将远远超过 330 亿美元。因此，这将是一次非常昂贵的攻击，在我们看来，成本可能高达 1000 亿美元。如果攻击得逞，以太坊当然可能会失败，但一些以太坊用户会在这一过程中变得富有。这种攻击对生态系统的影响将是巨大的，以太坊竞品的代币价格将出现大幅反弹。现在以太坊被摧毁了，投机者会试图确定哪种币将取代以太坊。更有趣的是，投机者会试图预测 Elizabeth Warren 下一步会投入到哪种 PoS 币。因此，这种攻击会适得其反，可能达不到 Elizabeth Warren 的目的。

接下来要考虑的是对手试图在 PoW 币中购买算力并达到 51%，以生产空块。要达到 51%，成本可能非常昂贵，而且需要相当长的时间，可能需要数年。这将涉及购买挖矿硬件、购买挖矿设施、购买电力以及雇用人员运营这些设施和维护挖矿硬件。重要的是要记住，新技术正在不断发展，新设施正在上线，新的 ASIC 正在制造，新的挖矿芯片正在研发。为了让对手达到 51%，可能还需要参与并资助芯片研发和 ASIC 制造。上述许多过程风险极大，执行风险也相当大。政府在管理这些风险和执行方面的效力和效率可能远不如私营部门。因此，政府可能需要比私营部门多花费很多才能有把握达到 51%。由于所涉及的复杂性和风险，政府可能需要花费至少是私营部门的两倍，甚至更多。在我们看来，这可能导致几年内的成本接近 1000 亿美元，与购买以太坊三分之一质押权益的成本差不多或略低，但执行风险可能比购买质押权益大得多。这是极其昂贵的。同样，这样做也会适得其反，因为这会造成大量的能源浪费，与 Elizabeth Warren 的表面目标未必一致。当然，政府的一个优势是，如果私营部门发现了政府的计划，私营部门可能会因预期投资回报率降低而减少开支，从而使攻击变得更便宜。

在这里，PoW 系统的一个关键因素是，攻击者可能需要长期持续花费资金来维护和维持攻击，而对于 PoS 系统来说，这主要是一次性成本。比特币极端主义者可以耐心等待任何攻击结束。攻击者最终可能会失去对算力的控制，网络可能会恢复。另一方面，在 PoS 系统中，一旦攻击者拥有三分之一的质押权益，也许他们就能永远杀死这条链。当然，也可能会有一个硬分叉来罚没攻击者的资金，就像 PoW 系统可以硬分叉来改变哈希算法一样。但假设没有共识规则的变更，PoW 系统的优势在于攻击者必须持续付出代价来维持攻击，也许是无限期的。这与 PoW 支持者认为的 PoS 系统的一个关键弱点有些相关，即缺乏与现实世界的锚定。

没收风险

Elizabeth Warren 可以采取的一种更可行的攻击方式是试图用武力或法律手段没收三分之一的质押权益或没收一半的算力。这种做法不在本文的讨论范围之内，本文的重点是探讨更典型的攻击形式的经济成本。不过，什么更容易被没收还是值得考虑的。就风险而言，从使用自己的物理硬件的小型自托管质押者那里没收质押权益，难度可想而知。转移质押权益就像转移私钥一样简单，而且很容易在不被发现的情况下跨境转移。这与挖矿硬件形成鲜明对比，后者在运输过程中可以被发现和扣押。另一方面，如果质押是通过受监管的托管服务进行的，这似乎比没收挖矿资产更容易。因此，不难理解，从根本上说，挖矿的安全性取决于挖矿资产是否分布在多个司法管辖区，矿场规模是否尽可能小。同样，质押的安全性取决于用户是否使用自己的硬件进行自主质押。

当然，如果 Elizabeth Warren 真的没收了大部分算力，这些挖矿资产可能会随着时间的推移而退化和恶化，而其他人则可以建立基础设施，这样网络总有一天可以恢复。相比之下，如果对手获得了 33% 的质押权益，那么 PoS 链就可能永远完蛋了。在 PoW 系统中，你至少有机会等待攻击结束，摆脱过去的负担，并恢复网络。

结论

一般认为，如果对 PoW 网络和 PoS 网络的攻击成本进行基本计算，PoS 网络的攻击成本要高得多。实际上，在对成本进行不完全的同类比较时，两者的差异比许多人预期的更小，质押权益系统的攻击成本仅略高。总的来说，我们的逻辑基于以下假设：要组织 PoS 网络，你需要三分之一的质押权益，而不是 PoW 网络的 50%；建立和维护算力比建立质押权益有更多的执行风险。综合起来，这些因素减轻了在市场上购买大量代币的较高成本。

无论人们如何看待 PoS 或 PoW 系统对经典经济攻击的抵抗力，为了使这些网络在资源充足的国家攻击下生存，挖矿资产和质押代理的分布是关键。不幸的是，以太坊和比特币在这方面都还有改进空间。从长远来看，抵抗审查可能取决于质押服务提供商的经济激励，以及全球范围内廉价、可靠能源的分布。