为什么以太坊2.0合并后对DeFi的攻击更难执行？

最近有人在讨论矿工是否有可能采用以太坊的一个修改过的客户端，这个客户端现在还不存在，主要是为了让矿工能够受贿。，区块链的短期重组(创建这种贿赂的主要用例是攻击DeFi协议)。在本文中，我们将解释为什么这种攻击载体在以太坊2.0合并后更难执行。

什么是分叉选择规则，为什么重要？

fork选择规则是一个函数，由客户端评估。这个函数将块集和其他看到的消息作为输入，然后输出&quot权威链&quot给客户。需要分叉选择规则的原因是，因为可能有多个有效链可供选择(也就是说，如果同一父块的两个竞争子块同时发布)。

reorg是这样一个事件，即原本属于权威链的——个块不再成为权威链的一部分。因为竞争对手打败了它。最终确定的是，——的分叉选择规则强有力地支持了某个块，使得该块在数学上(或至少在经济上)无法重组。

在某些分叉选择规则(如Tendermint)中，重组是不可能的；分叉选择规则仅通过添加BFT(拜占庭容错共识协议)同意并最终确定的任何块来扩展现有链。

以太坊的现状如何

。在其他分支选择规则中，重组非常普遍。

我们通常看到的是&quot最长链规则&quot(或者，更准确地说，是&quot最大总挖掘难度规则&quot)在以太坊这样的权力区块链。这意味着当客户看到两个区块链时，，它将选择总难度最高的一个(即链中所有块的总和)。

为了举例方便，假设方块难度可以是100或者110，想象以下场景：

1。我们从难度为100的块1开始同步。

2、方块2a和3a都以100的难度到达，我们将它们嵌入到我们的区块链中形成一个总难度为300的分叉。

3。块3b以难度110到达，并声称2a是其父块，形成一个总难度为310的分叉。分

叉选择规则将发现当前&quot最重&quot链式是第二叉，然后选择它代替。这种情况属于一个街区的重组。因为只有块3a被改变。请注意，该块不是直接丢弃的，因为新到达的块可能会导致分叉选择切换到第一个分叉。

4，2b块和3c块都是难度110到达的。，形成总难度320的新分叉。这意味着fork选择规则现在将使用2b而不是2a，3c而不是3b，并且块2a和3b都在最后的授权链中。这次重组属于两个板块。

读者应该能够看到逻辑是如何发展的。如果一个新的块4a到达并声称3a是它的父块，那么分叉选择规则将被改变以选择第一个分叉，依此类推。延迟引起的

链重组

的影响短期重组经常发生。矿工A和矿工B可能同时找到一个有效的块，但是由于该块是在p2p网络中广播的，所以一些网络可能会看到矿工A&#039s块第一，而其他人可能会看到矿工B&#039；s街区第一。如果两块难度相同。，将有一个抽签，客户将随机选择或选择首先看到的块。通常情况下，当第三个矿工C在矿工A或B建造的积木上建造积木时，另一个积木会被遗忘。偶尔运气不好会导致2-5块重组。。比这更长的重组时间几乎总是由于极端的网络故障、客户端漏洞或恶意攻击。

短程重配置并不致命，但确实给网络带来了一些严重的有害后果：[XY002][XY001]节点开销：当一个重配置一起发生时，因为需要切换到新的fork，所以可能需要重新执行事务或状态编辑，节点会有一些内存和磁盘开销。

用户体验下降：可能的重组意味着用户需要等待更长时间才能安全地处理需要&quot已确认&quot。。这方面的一个重要子用例是，交易平台等公司需要等待更长时间才能接受存款。

事务背景的不确定性：当用户发送一个事务时，他们会更加不确定该事务将在哪个上下文中执行(例如，最新的n个块将被回滚)。显然，这将使DeFi交易更容易出现意外的失败，比预期的交易结果更糟，或有害的MEV提取。

更易遭受51%攻击：在以最长链为分叉选择规则的系统中，如果区块链从B1重组，那么B1的难度不再为链提供安全性。攻击者不再需要击败所有诚实的矿工。他们只需要击败那些没有被重组的诚实的矿工。如果经常进行重组，那么攻击就会容易得多。

可能的最坏情况

在最坏的情况下，频繁的重组将使区块链结算担保完全失效。并阻止它继续。通常，对于砌块制造商来说，&quot激励相容&quot应该是延长最长的链但是如果一个块执行后的状态是极其有利可图的(比如交易成本很高，或者MEV只能通过直接在块后新建一个块来提取)怎么办？。这个问题在过去讨论&quot没有区块奖励的比特币&quot和自私的挖掘，但这也已经在今天讨论过&#039；s&quot以太坊生态学中与DeFi相关的&quot。

在所有这些情况下，都有强烈的动机试图通过与其他区块竞争来窃取费用，而不是扩展授权链。在下面的例子中，区块1的执行后状态非常有利可图，区块2a已经被挖了。然而，它不是一个相反，三个阻挡者选择继续在区块1而不是区块2a上挖掘(以获得区块1后暴露的MEV)，这可以扩展到任何数量的阻挡者。

很明显这种模式为51%的恶意攻击打开了方便之门。我们称矿工&#039；参与此次矿业战略重组&quot短视的理性&quot因为短期内决定这样做可能是理性的。但是，他们都或明或暗地(矿工)看好ETH(因为交易费和大宗奖励都是以ETH计价的)，这意味着这种减少用户的攻击&#039；对以太坊的信任与他们的最大利益相冲突。所以，长期来看是非理性的。

合并的PoS以太坊

在NakamotoPoWconsensus算法中，块是&quot持续地&quot在分叉选择中最终确定。第一，挖一块的时候。这个时候，一个竞争区块或许可以对其进行重组。如果一个区块被成功打包到授权链中，其他矿工将在(平均)13秒后在该区块上建立第二个区块。此时，如果要重组一个链，它需要两个竞争块。随着越来越多街区的建设链条重组的难度会不断上升，但速度很慢。

以太坊信标链实现了一个名为Gasper的权限证明协议，它的分叉选择规则被称为LMD-幽灵。不像中本聪。在Gasper中，区块涉及两个角色：

提议者：负责提议区块的验证者

证明者：由一组验证者组成，他们对应该是权威链头的区块进行投票。。认证者的投票被称为&quot证词&quot，也就是&quot重量&quot他们给了街区。控制证明者意味着控制分叉选择规则。

每12秒有一个时段，代表一个提出区块的机会。。在每个时间段，将有一个洗牌算法来随机选择一个委员会，该委员会由大约1/32的所有验证者组成，其中每个委员会中的一个验证者将是提议者，其余的验证者将是证明者。。证明者还对他们认为

应该打包到权威链中的块进行投票。因为委员会是由伪随机抽样组成的，所以攻击者没有办法将他们所有的验证器集中在一个槽中。

目前信标链中大约有196，000个验证器，这意味着每个时隙中的委员会数量大约为6125个。因此，即使是重组一个区块也是极其困难的。因为一个只控制部分验证者的攻击者，是无法打败成千上万诚实的多数验证者的。

为了更好地理解为什么会这样，让&#039；让我们看看下面的例子：有2个插槽和24个验证器，其中9个是恶意的。。核查员分为两个委员会，随机洗牌后，对手不太可能控制他们分到的50%的委员会成员，更别说重组了。

更正式地说具有p%承诺的恶意行为者控制超过50%的n个验证者的大小委员会的概率遵循二项式分布(其中k=n/2):

。

算出多个质押值的概率后，我们得出下表：

现在我们知道，攻击者要想直接重组，需要控制验证者总数的50%。

如果控制者控制了25-49%的证明者(见本文或这里的摘要)，控制者仍有可能发动一些较小的攻击。但是这些攻击已经被修复，可以安静的执行，从而达到近50%的无条件安全。

最后，长期重组是不可能的，因为所有比过去两个时期更深的块都将被视为&quot最终确定&quot。换句话说，回滚它们是不可能的。如果最终确定了一个攻击者造成的两个冲突块(比如控制了质押金额的67%)，则系统需要回过头来通过社会干预进行恢复。

带有重组策略的博弈论

现在我们知道了在不同的分叉选择规则下重组是如何发生的，我们不妨从一个简单的博弈论例子中学习一下，什么时候矿工或验证者运行软件来执行重组以获取利润是有意义的。

我们可以用收入矩阵非正式地描述每个场景，其中&quot兵变&quot意味着&quot下载并使用执行重组的软件&quot。好处是&quot目光短浅&quot而不考虑长期后

果。中本聪

在最长链PoW中，即使是验证者集合中的少数人也可能实现短程重组。实现后利润极高的区块总会偶尔出现，即使成功的概率是1-10%，也值得尝试与这个区块已有的子区块竞争。

矿工可以组成一个中等规模的矿池，等待未来连续找到2-3个区块的机会，或者将他们的部分收入发送到一份合同，任何人都可以声称贿赂其他矿工运行相同的软件来构建他们的区块链。帮助它击败现有的权力链。

因此，一些矿工可能会尝试运行重组客户端。

Gasper

在Gasper中，可以重组1-64个插槽，但是攻击者需要控制整个验证器集的大部分(因为他们可以&#039；不要将他们的存款集中在特定的位置)所以他们的认捐需要足够大，以便在他们想要攻击的槽中随机选择)。除非大量其他验证者也同时使用，否则采用重组挖矿软件用处不大。

因此，如果51%的验证者有一点利他或者偷懒，基本可以肯定没有人会去运行重组挖矿软件。

Tendermint

在Tendermint中，事情会更简单：重组是完全不可能的，任何违反单个槽终结规则的实现都需要没收三分之一以上的验证器。类似于加斯伯&#039；的情况这也意味着，基本可以确定，重组挖矿软件不会有人运行了。

从上面我们可以看出虽然有可能采用&#039；重组geth&#039在这三种情况下，基于平行证明概念的分歧选择规则比Nakamoto分歧选择规则带来了更稳定的诚实平衡。

总结

在以太坊的背景下，最有效的预防措施是进一步加快合并，特别是培养达到可接受的&quot紧急合并&quot从而将以太坊转化为PoS机制。仓促的合并会带来高风险

，破坏基础设施。但是，如果许多矿工开始重组链条，他们仍然需要一个可信的承诺来抵制这种行为。当合并临近时，风险是最大的，因为矿工们仍然主宰着这个系统，但是他们的时间不多了。然而有两个因素会减轻这种风险：

以太坊矿工通常是(I)同时在其他区块链的矿工，和/或(ii)拥有其他能力的以太坊社区成员，因此表现良好的机会继续存在。

随着并购的临近，紧急并购的成本和风险都在降低。在预期的合并日期前几个月进行紧急合并是非常具有破坏性的。预计合并日期前两周的紧急合并可以为验证者操作员已经下载的客户端提供参数设置。

合并后，重组验证将成为一个更小的问题，因为单个验证者或一小组验证者无法独自重组一个区块。一个成功的重组攻击需要解决大多数验证者同时参与的协作问题。但是，还是有一些小风险。。如果想进一步提高安全性，那么以太坊要么可以进一步调整分叉选择规则，将重组攻击的要求提高到理论最大值的50%；或者转而直接单槽达成最终共识。

Acknowledgement:ThankstoDanRobinson,AnishAgniHawtrey,KevinPeng,DaveWhiteandMeiWenTengfortheircommentsonthisdraft

.