以太坊被认为是所有加密货币中最去中心化的一层区块链。然而，美国财政部外国资产控制办公室(OFAC)最近的进展可能会破坏以太坊的完整性&#039；反审查。第一OFAC批准了龙卷风现金和其他几个相关的以太坊地址。受监管的美国实体和各种DeFi应用程序迅速遵守这些制裁措施，并将OFAC指定的地址列入黑名单。

以太坊向股权证书(PoS)的过渡将ETH质押集中在四个主要参与者：丽都、比特币基地、北海巨妖和币安。这些集中的参与者需要遵守美国的法规。，并服从OFAC的要求，如审阅地址。这些发展极大地破坏了以太坊去中心化的完整性，同时也引起了加密界的密切关注。

集中ETH质押市场份额问题

以太坊的一个关键集中指标是提供商承诺的市场份额。不考虑OFAC，市场份额集中在大型质押提供者之间，这将导致串通的可能性。主导不良行为者合谋改变新的交易秩序。并检查特定的块或地址。由于丽都、比特币基地、北海巨妖和币安占据了ETH总市场份额的58.8%，因此需要担心ETH质押提供方市场份额的过度集中。

2022 年 8 月 8 日美国财政部将隐私协议TornadoCash列入其制裁名单，声称网络犯罪分子利用加密货币项目进行洗钱活动。比特币基地、北海巨妖和币安等集中交易所很快遵守了制裁措施。，并将与龙卷风现金相关的以太坊地址列入黑名单。

虽然集权实体需要遵守法律法规，但龙卷风现金制裁凸显了集权实体控制以太坊的潜力。这就提出了一个问题。如果财政部命令这些公司利用其占主导地位的质押市场份额，进一步审查以太坊基础层面的交易，有什么可以阻止他们？

以太坊等区块链的绝对核心目的之一是提供中立性和审查阻力。对以太坊反审查能力的威胁，就是对去中心化核心前提的威胁。OFAC

为了全面了解可能的审计，您需要知道哪些验证机符合OFAC标准，或者哪些验证机使用符合OFAC标准的中继器？

资料来源：MevWatch

大多数验证器运行一个名为&quotMEV-Boost&quot。简而言之，MEV-boost允许PoS验证者将批量生产责任外包给出价最高者，从而有效提高验证者的APR。。MEV-boost提高验证者APR70%，验证者很难忽略。

上图追踪了自合并以来MEV-boost中继器建造的符合OFAC标准的区块的百分比(占MEV-boost建议区块或所有区块的百分比)。。以太坊生产的63%的合并块符合OFAC标准。这意味着，如果OFAC兼容验证器停止证明非审查块，它们将最终形成一个100%审查的规范链。

最流行的中继器是由Flashbots开发的，符合OFAC标准。目前，验证者可以从八个中继器中选择：

Flashbots(OFAC兼容)

。

EdenNetwork(inlinewiththestandardsoftheOfficeofOverseasAssetsControloftheUSTreasury)

Localmachine(inlinewiththestandardsoftheOfficeofOverseasAssetsControloftheUSTreasury)

bloxrouteregulated(inlinewiththestandardsoftheOfficeofOverseasAssetsControloftheUSTreasury)

maximumprofitofbloxroute(notmeetingthestandardsoftheOfficeofOverseasAssetsControloftheUSTreasury)

BloXrouteethical(notmeetingthestandardsoftheOfficeofOverseasAssetsControloftheUSTreasury)

Manifold

relayooor

在激活MEV-Boost的验证者中，由MEV-Boost中继的94%的块正在实施OFAC合规性。这意味着在协议层面存在审查，不利于权力下放。

资料来源：MevWatch

可以提出一个有效的论点，就是龙卷风现金可以帮助不良演员匿名，所以相关地址被列入黑名单是正确的。但是，这忽略了所有出于隐私原因使用龙卷风现金的好演

员。。最令人担忧的是，OFAC有权决定什么是合规的，什么是不合规的，并迫使合规的实体遵守。OFAC合规性将网络置于不稳定的位置，验证者正在提交集中式实体的请求，从而威胁到以太坊的一个核心特性。，也就是放权。

防御机制：社会砍杀

VitalikButerin等开发者认为，以太坊仍然有一张王牌：实现用户激活的软分叉(UASF)——的可能性，这是一种社交缩减的形式。在他的博客中，Vitalik描述了UASFs如何阻止51%旨在审查的联合攻击。UASF是一种机制。区块链节点通过这种机制激活软分叉(网络更新)，而无需从链的区块生产者(证据中的验证者)获得通常的支持。在UASF的比赛中，大多数攻击者&#039；在以太坊，这是通过&quot不活动泄漏机制&quot).没有明确的&quot硬分叉删除货币&quot是必需的。除了需要在UASF上协调以选择几个块之外，其他一切都是自动完成的，只需遵循协议规则的实现。

所以攻击者第一次攻击链会花很多钱，以太坊几天内就能顺利恢复。。再次攻击该链需要攻击者获得新的令牌来替换被破坏的令牌。如果他们再次进攻，他们会损失很多钱.又来了(你懂的)。这个游戏非常不对称，对进攻方不利。UASF是如何在以太坊工作的？

社会还原不是迁移到权益证书后内置到协议中的流程，所以需要UASF。以太坊会把违规的减少限制在非常具体的行为。。任何实现协议级标准以进一步减少犯罪的行动都需要通过以太坊的进一步升级来实现。UASF的基本原理如下：

验证者遵守OFAC，开始审核交易

以太坊社区不同意。验证者被切断

验证者要么改变其行为，要么离开以太网。

现在考虑像比特币基地/北海巨妖这样的美国实体。如果这些公司想在美国经营质押服务，，你必须遵守OFAC的规定。如果ETH用户试图利用UASF对抗OFAC的审查，符合美国标准的验证者(如比特币基地/北海巨妖验证者)将需要遵守OFAC。在这种情况下、比特币基地或北海巨妖验证器将被剪切。问题是，比特币基地和北海巨妖正在运行质押池，持有激活UASF的用户的ETH存款。

黑色标志

以太坊的一些用户中的黑旗运动宣布他们愿意支持手动分叉(UASF)来对抗试图实现系统范围审计的验证者。

相反，生态系统的参与者不会&#039；我不想砍掉像比特币基地这样的中央集权实体，因为它是零售之都。。但是，审查制度要像双花攻击一样严肃对待。如果有人双花，他会被剪，如果有人审查，他也会被剪。UASF是任意的，没有编码或自动化，取决于人类的决策。。什么样的审查制度值得大大减少保留用户的中央集权实体&#039；代币？这就是社会还原的争议。让事情变得更复杂的是，以太坊社区不能依靠一个像维塔利克这样的领导者来发起UASF。。依靠一个&quot网络霸主&quot会导致另一种形式的集权。

展望未来，比特币UASF是UASF的成功范例。比特币网络的核心开发者其实并不&#039；不支持比特币UASF，但退居幕后，让社区来决定。。归结起来就是社区推动社会减叉。UASF公平运作的唯一途径是通过基层方法。

SWIFT的经验教训

ErikWall强调Swift在其网络中传输的报文不受OFAC法规的约束。SWIFT是一个跨辖区的银行报文网络。如果您必须遵守每个司法管辖区的OFAC法律法规那你就&#039；没有像Swift这样的跨辖区报文传送层。你可以&#039；不要同时遵守每个司法管辖区的规则，这就是为什么你可以&#039；不要对全球系统进行网络级审查。这条线赢了&#039；t工作。如果连斯威夫特都不知道。不遵守基本的OFAC规则，以太坊为什么要遵守？