

近日，美国财政部发布《去中心化金融非法金融风险评估》(以下简称“评估”)。

此评估是对2022年9月白宫数字资产框架的回应。该框架特别要求财政部对分散融资进行风险评估。根据美国财政部的说法，单词“DeFi”在虚拟资产行业中经常被滥用，并列出一一些非法金融风险。

不过，最值得注意的是，财政部认为DeFi活动应当履行《银行保密法》(BSA)的反洗钱(AML)义务。这是我们第一次看到美国政府对DeFi如此强烈和鲜明的态度。最后，评估寻求行业参与。为了了解权力下放领域中可行的合规形式，特别是如何鼓励DeFi服务实施某种形式的“反洗钱”控制。

这份评估包含了迄今为止美国政府对DeFi最全面的讨论，并提出了一个观点。也就是说，即使是真正的(或多或少的)分散服务也应该实现“反洗钱”合规运营。在某些方面，大力推行传统的“反洗钱”顺从与DeFi的发展是相悖的。DeFi依赖于非中介软件，而不是合规团队。

【xy001】以下是评价的重点内容：【xy 002】【xy 001】(1)定义很重要【xy 002】【xy 001】在DeFi领域，关于定义的讨论很多，因为分散金融的形式有很多种。

在金融行动特别工作组(FATF)于2021年10月发布的指南中，全球“反洗钱”标准制定者提出了“所有者/经营者”测试。人们认为“拥有控制权或影响力的创造者、所有者和经营者”应该是有反洗钱义务的虚拟资产服务商，即使项目看似去中心化。FATF在DeFi和AML的第一次讨论中指出“控制”包括对项目进行控制或与用户保持持续的关系。

财政部借鉴FATF的观点，并指出：“目前，即使在行业参与者中，也没有普遍认可的DeFi定义。或就能使产品、服务、安排或活动的特性达成一致”；分散”；财政部解释，该术语广泛用于指通过使用自动执行软件实现点对点交易的协议和服务。财政部与FATF相同，试图区分真正的去中心化的软件和只是简单的宣称DeFi但实际上拥有中心化属性的实体。

虽然评测在定义上投入了大量的时间，但是并没有得到一个明确的定义。服务是分散的吗？，或者“只是名义上的赤字。仍然是个例。在确定监管义务时，这种案例审查将变得非常重要。

(2)重要消息：部分DeFi服务可能存在BSA规定的反洗钱义务

评估报告指出，美国 # 039；反洗钱义务以活动为基础，并声称BSA要求像金融机构一样运作的实体 # 39；建立并实施有效的反洗钱计划 # 39；遵守对OFAC的制裁。财政部声称。虽然一个人的集权程度可能会影响他提供的服务。然而，从事BSA所定义的金融机构活动的人，无论是集中还是分散的，都将有这些义务。

上面提到的这一点很重要。 ，因为它可能会将完全基于软件的DeFi服务与拥有合规团队和履行反洗钱义务所需的其他资源的大型金融机构归为一类。

### (3)犯罪分子还需要提取资金

评估列出了DeFi生态系统中的一些非法融资风险。这些风险本质上与集中式加密中的风险相同。报告指出了洗钱、勒索软件、盗窃(如闪电贷款和黑客攻击)、杀猪菜等骗局。在洗钱中，现象 # 39；DeFi服务 # 39；如跨链桥，分散交易所(DEX)，硬币搅拌机和流动性池被用来洗钱进行了评估和讨论。换句话说，评估报告说DeFi在洗钱过程中被用来对非法资金进行分层。然而报告确实指出，——与我们在链中看到的一致。——非法行为人依靠集中交易所回笼资金，并将其转换为更可用的法定货币。换句话说，对于洗钱， # 39；条条大路通VASP # 39；。中央集权的VASP必须实行 # 39；反洗钱 # 39；控制，那些没有这样做的VASP，以及他们的国家，是监管机构和国际标准制定者的目标。

报告中强调的DeFi的一个重大漏洞是DeFi生态系统中黑客和盗窃的激增。根据TRM的数据，2022年是黑客攻击创纪录的一年，约有37亿美元被盗。对DeFi项目的攻击尤其常见。大约80%的被盗资金(30亿美元)影响了DeFi用户。跨链桥黑客攻击的规模是其他攻击的15倍。然而，我们也看到区块链的情报工具和事件响应程序在追踪DeFi生态公司被盗资金方面变得越来越先进。

### (4)降低风险有一些方法

虽然评估的重点是风险，但确实要花很多时间来研究如何降低这些风险，包括使用当前 # 39；反洗钱 # 39；监管框架(如BSA)和在全球范围内实施FATF标准。 。虽然报告指出，公开区块链允许更大的透明度，可以在金融犯罪调查中使用区块链情报信息，但财政部表示，调查受到钱包和交易匿名性的限制，很难将它们与现实世界的实体联系起来。财政部认为货币混合器的应用和加密货币的匿名性加剧了这一点，但与此同时，像TRM这样的区块链情报工具也在随着这些新兴技术的发展而不断发展。

财政部指出，潜在的技术解决方案可以降低风险。 ，如区块链智能工具、数字身份和零知识证明， # 39；潜在的解决方案旨在支持履行反洗钱/CFT义务的各种要素

，同时最大限度地保护用户隐私，包括通过数字身份技术支持DeFi服务的身份验证。 ，可由用户验证& # 039；区块链的交易历史。【xy 002】【xy 001】(5)财政部呼吁各方共同努力【xy 002】【xy 001】虽然报告的大部分内容都是关于风险和漏洞，但在最后几页呼吁美国政府与业界合作。 ， &quot进一步阐明如何将适用的法律法规应用于DeFi服务& quot，并根据反馈给出进一步的指导。财政部还呼吁继续研究技术的持续发展，私营部门的参与，并关注DeFi领域的网络灵活性。此外财政部还呼吁美国政府与开发工具以推广创新解决方案的私营实体合作。

报告中的建议总结如下：

加强美国虚拟资产活动的反洗钱/反恐怖融资监管。

评估适用于DeFi服务的美国反洗钱/反恐怖融资监管体系的优化可能性。

继续研究并增加私营部门的参与，以支持对DeFi生态系统发展的理解。

继续与国外合作伙伴合作。

倡导加强虚拟资产公司的网络灵活性、代码测试和强大的风险信息共享。

促进负责任的风险降低措施的创新。

## 结论

虽然美国财政部明确表示，风险评估不& quot设定新的监管预期& quot，但它为我们了解美国财政部如何看待& quot反洗钱& quotDeFi生态系统中的义务，并概述了在真正分散的领域中的作用。 ，一个更广泛的关于谁来监管和如何监管的全球讨论。

风险评估报告确实达到了预定目标，即评估风险。但同样重要的是，要认识到DeFi给金融业和打击金融犯罪带来的机遇。 。TRM的Ari Redbord在最近的CFTC技术咨询委员会(TAC)会议上的开幕词中强调了这一点。简而言之，就像阿里说的那样。DeFi已经实现了一个点对点金融服务的生态系统。 ，摆脱困扰我们现行体制的诸多问题。以互联网的速度进行点对点的跨境价值转移。这是一个承诺。正如报告所认同的，区块链技术也有能力提高金融犯罪合规的有效性。因为监管机构现在有能力在防篡改账本上实时查看金融交易。