原文标题：《a16z 给监管者的一份信：你们应该如何恰当地监管DeFi？》原文编译：吴说区块链

摘要

本文是a16z为金融稳定委员会(FSB)“加密资产活动的国际监管”主题活动撰写的评论信，主要分为三个部分。[ xy 002 ] [ xy001 ]1.讨论差异，相应的DeFi监管框架应该如何参与web3APP应用而不是Web3协议的监管(监管企业而不是软件)

2.在讨论隐私重要性的同时

3.注意不要制定过于严格的法规。
因为这些法规运行良好，禁止过度抵押的算法具有稳定货币的效果。
建议降低对抵押品的要求风险。
这是因为运行良好、禁止过度抵押的算法有可能稳定货币。
我们认为抵押要求可以降低风险。[ xy 002 ] [ xy001 ] fsbfinancialstabilityboard金融稳定委员会成立于2009年4月，是专业的国际组织负责世界金融体系的监管和建议。 作为2009年20国集团伦敦峰会成立的金融稳定论坛的继承者，其成员当然包括20多个国家的中央银行、财政部和金融监管机构以及各主要国际金融机构和各专门委员会。

去中心化金融DeFi

CeFi和DeFi的区别

很多人把“加密CeFi”和DeFi混淆了因为两者都是顾客和用户参与加密市场的手段。 但是，CeFi和DeFi的结构根本不同。
我们认为，正因为有其自身的特点，才需要各不相同的监管框架。 首先，CeFi机关正如其名、“中心化”运营，与完整的管理团队存在利益冲突，用户与第三方中介机构对话进入加密市场。 中介机构通常是传统的民营企业，用户是企业的客户，如何经营企业的决策是在关门的过程中做出的。
另一方面，DeFi由软件合同组成，提供许多非中介金融产品和服务。
这些软件协议通常由为实现区块链中心化而引入的智能合约集合组成。 用户无需中介就可以直接与这些协议进行交互，通过点对点交易来交易金融产品，管理DeFi协议的规则是用计算机代码编写的，在计算机代码中执行。 在金融管制过弱的司法管辖区和/或对政治、金融或机构信任受损的司法管辖区，这一点尤为重要。 透明交易和链上风险的释放将降低不透明杠杆化的可能性，在更透明的相互联系层面加强风险管理，也有利于避免金融感染风险。[ xy 002 ] [ xy001

]因为defi依赖代码而不是中介所以DeFi协议非常透明。
一般来说，任何人都可以检查和审计公共链的账目。 许多DeFi协议建立在这些公共链上，这些公共链的账簿反映了管理协议操作的智能契约、以及输入到特定平台的每个交易的价格和数量的记录。 例如，典型的DeFi贷款合同Compound具有透明、不变性和可公开检查的所有历史交易账簿。 重要的是这些信息几乎是实时的。与

相比，由于CeFi的中介机构不透明，公众只能获得有限的零星且事后所需的信息。考虑到使用开源代码和在链上跟踪的DeFi系统的透明度，监管机构和用户可以相对容易地进行监控CeFi中介机构无法实现那个。 迄今为止，DeFi协议对市场压力表现出显著弹性，尤其是与CeFi中介机构进行比较。
在最近几个月的市场波动中，加密市场的大规模破产集中在CeFi机构像Celsius Network和Voyager Digital那样，没有真正中心化的DeFi协议，如Compound、Uniswap都可以正常工作。
这种相对成功既是DeFi协议智能合约完整性的功能，也是透明性的功能。 考虑到这些优点，我相信DeFi生态系统在未来几年在使用、实用和复杂性方面将继续发展。

DeFi的新监管框架：监管APP应用

如上所述，针对DeFi定制的合适的监管框架是中心化/业务专有APP或合同的不是协议或软件本身。
如下所述，业务拥有的APP应用程序和协议之间的差异很重要。

DeFi协议

DeFi协议是由智能协议构成的软件程序为点对点贷款和其他金融交易提供功能。 协议承载在块链上，或者集成在以太网等块链中，具有开源、中心化、自治、容错性。 在这些特征中，去中心化和抗审查具有特殊的监管和政治意义。 去中心化是一个广义术语、政治/法律中心化(因为没有人控制公共链)和体系结构中心化(因为没有中心障碍点)等区块链的多个方面。

正如许多监管机构指出的，去中心化是一个范围，部分web3业务从中心化开始，转向去中心化模式。 我们建议存在“充分”的中心化web3实体。 其中(I
)关于其运营的信息是透明的，对所有人都可用)通过透明的区块链账簿实现。、(ii
)不需要或不需要推动企业成功或失败所需的管理努力)
)通过一成不变的智能合约、去中心化经济和经销实现)。

抗审也是一个广泛的术语描写了几乎谁都可以使用锁链的能力和没有人会被赶出锁链的事实。 区块链上还描绘了这样一个事实，即没有人能独立强大到阻止交易或阻止希望验证区块链交易的其他人加入协议网络。

由于无人管理协议，协议不能包含传统金融法规有时要求的主观决定，因此无法遵守或理解特定的司法要求。 例如，证券、大宗商品、各种衍生工具等产品分类因司法管辖区而异各国之间可能有很高的主观性。
全局可访问软件不能应用事实和环境测试，也不能在编程中包含不一致性。 此外，无论法律和法规如何变化，部署DeFi协议(如Uniswap协议)时中选择所需的族。
通常，设计参数会大大限制功能的更新，因此它会像最初创建的那样永久运行。 如果web3社区投票支持更新为新版本的DeFi协议或启动新版本的协议，则在向用户提供对早期版本的APP应用程序的访问权限时，将更新代码库单击，指定新版本的智能合同。 [ xy 002 ] [ xy001 ] DeFi APP解释[ xy 002 ] [ xy001 ] defi APP解释是建立在defi协议之上的产品，它允许用户访问这些协议。
重要的是通常添加连锁或连锁订单数据库、图形用户界面(GUI )和/或API。
与协议层不同，web3APP应用的业务和开发者在主观决策上没有相同的约束。 它们可以遵守各种司法法规，并设计灵活的访问门户，将法律和监管风险降至最低。

传统CeFi法规不适用于defi，因为为DeFi

cefi设计的法规不能很好地解决两种产品和服务之间的差异。
在CeFi领域许多法规旨在消除信任金融中介机构的风险。
目标是降低潜在的利益冲突和直接欺诈的风险。
如果一个人必须把钱或资产托付给另一个人，这就可能发生。
在DeFi的世界里传统的金融服务是中介化的，没有可靠的中介。

因此，区块链技术的集中化、透明度和可靠性消除了DeFi中许多CeFi法规主要以解决问题为目的的风险。 于是，我决定、DeFi可以将用户与CeFi盛行的诸多渎职行为隔离开来，优于CeFi的任何“自我管理”或“公共管理”制度。
于是，我决定中选择所需的族。
将CeFi法规大规模应用于中介服务这样的非中心化web3APP应用是不合逻辑的。

此外，任何监管干预都是相反的因为它阻碍了德福I实现许多金融监管要求的非常合理的政策目标的原有能力，例如透明度、可核查性、可追溯性和负责任的风险管理。 想象一下强迫SMTP电子邮件合同遵守从言论自由法的执行到GDPR等数据隐私法等各种司法制度会造成多大的价值破坏？ 但是，访问SMTP并相互通信的APP应用程序可以遵循以下Gmail能够遵守各种法规要求，满足法规信息要求。
协议层面的传统监管做得不好。

合适的监管框架对于保证DeFi的利益至关重要

我们还认为，监管APP交易而不是协定原则也很重要对于保证DeFi对国际金融体系的透明度和可靠性至关重要。 如上所述，defi APP应用在区块链技术上运行，因此

可以向世界各地的任何人开放访问，为访问金融服务带来了前所未有的机会。 2020年1月以来，DeFi的用户数急剧增加，用户数从约9.1万人增加到近500万人，在可能损害对政治当局和金融机构信赖的新兴市场，DeFi的好处最明显。
拉丁美洲国家在采用DeFi方面处于世界领先地位，特别是在信贷设施不足的地区。 DFI也在尼日利亚和肯尼亚等非洲国家取得了进展。

如果采用监管框架来捕获驱动web3生态系统的软件基础架构，而不是用作接口盒的APP，则可能会危及数百万的开发商的DeFi利益，从而对合同开发商进行监管。 如果监管机构试图对web3协议实施主观和潜在的全球冲突监管，则无法实现中心化，例如什么是可能的、什么不是证券、商品或其衍生品等，从而损害了DeFi协议的功能和有用特性。 我们相信、国际官员和监管机构通过促进DeFi行业负责任的发展，特别是通过建立基于规范DeFi应用的明确可行的法律框架，能够最有效地应对这一挑战。

隐私与减少非法金融和国家安全风险

建立明确、一致的全球监管框架，以提高金融信心，打击洗钱和恐怖主义融资，对数字资产行业的成熟至关重要。 如果公共部门和私营企业积极合作，实时共享信息在减少洗钱、恐怖主义融资和其他非法活动的风险方面，这样的框架将是最成功的。

我们赞赏金融行动特别工作组(FATF )就数字资产领域的反洗钱(AML )和反恐融资(CFT )提出和指导的意见。 由于该部门不断创新，FATF必须继续与民营企业协商，其成员参与技术实际实验制定最有效地实现所需目标的政策，同时避免过于广泛或意想不到的后果。 此外，地方监管机构在实施FATF虚拟资产标准时，应当与数字资产行业进行类似接触。

美国，许多加密货币业务受到美国《银行保密法》的保护，这些受保护实体成功地从传统金融机构的“反洗钱”计划中受益，还开发了反映加密货币独特情况的附加要素。 另外、美国金融犯罪执法网络(FinCEN )与加密资产服务提供商密切合作，利用先进的信息和威胁检测能力。 但是，如果适用，“了解客户”（“KYC”)规则将应用于目标，并且必须使用区块链技术的技术力量。 应鼓励收集可识别用户数据的最小KYC流程，并使用例外补救和监管沙箱对技术和流程进行实验。 这种灵活的方法可以促进加密本机工具的开发，利用区块链技术和透明度有效打击非法金融。

所涉实体具有这些重要的合规义务，但隐私是基本人权和社会公益。 隐私保护技术允许有针对性地计算和分析数据，并对执行计算的人和试图窃取或破坏信息的恶意行为者进行加密。 零知识证明和可配置隐私区块链是隐私保护技术的新形式，可以

平衡隐私利益和更广泛的公共政策和社会需求，包括有效合规、透明和安全。

各国政府应采取法律和政策允许开发和使用保护隐私的技术的同时，也可以遵守这些技术。 例如，监管机构可以建立评估用于创建和维护数字身份记录的新机制的流程，包括采用数字身份验证技术该技术可以同时使用分布式区块链技术和安全链下的“数据存储”。 此外，零知识证明技术可用于制裁筛查。

同时，政府本身也应该尊重隐私只有在实现特定、狭义、合法的政府目标所必需的情况下，政府才能访问或使用个人数据。 例如美国财政部考虑收集、验证和保留在加密货币交易平台和非托管钱包之间交易金额超过3000美元的所有交易方的姓名和物理地址，这引起了严重的隐私和安全问题。
另外，这些建议可能损害执法人员的调查、起诉和资产追回能力。 这是为了将钱包用户从管理良好、合规的交易平台和金融中介机构驱动到不受监管或不受监管的实体，以减少执法和国家安全部门有价值的信息数量

最后，FSB建议澄清GSC报告高级别建议5中的声明。 也就是说，“当局必须确保GSC实施适当的反洗钱/反恐融资措施，满足FATF标准、包括遵守FATF旅行规则的要求”，具体研究GSC安排是否允许无托管钱包的点对点交易，仅适用于有旅行规则义务的覆盖实体。
它通常不涵盖非托管或非托管的钱包提供程序、用户或非VASP实体。

算法稳定货币

FSB对稳定货币的建议是，储备资产与发行人发行的稳定货币数量“至少”相等，仅由“保守”资产组成，稳定货币由算法推导而来，这会给区块链生态系统带来负面的意外后果。
更确切地说，我们担心这个基于提案的框架会有效地禁止算法稳定货币。 其中，最好的算法稳定货币在外生抵押品的超额抵押中发挥作用对依赖算法开发产品和服务的web3APP应用程序表示敌意。 我们衷心支持防止稳定货币发行者承担不合理风险的监管，但我们相信立法者可以在没有如此广泛禁令的情况下保护用户。 这可以通过制定允许开发安全软件代码但防止高风险项目的严格定制的抵押要求来实现。

算法不是问题

稳定货币是加密货币其价值与美元和黄金等外部资产的价值相关。 稳定货币可以通过集中管理担保和资产，或者通过使用与算法清算机制不同的加密货币或其他资产组成的担保的组合来维持挂钩。 一般来说、立法者和监管机构通常关注使用算法的稳定货币，即算法稳定货币，将其作为风险领域。 但这种过于广泛的担忧大错特错，因为我们关注算法作为不稳定的来源，而不是抵押不足的真正问题。

在当前市场波动持续近一年的时候，我们发现目前几乎所有的算法稳定货币项目都非常好，但极少数不顺利项目的抵押品严重短缺，它们依赖于发行人自己创造的抵押品重要的是，通过算法货币相对安全的原因是区块链的可编程性，建立了传统清算基础设施的一些典型的关键风险控制，包括抵押品清算，从而保护投资者和协议的安全性和稳健性，比手动过程更

区块链可编程性的一个例子涉及稳定货币，要求用户向ETH收款作为抵押品。 这些协议要求ETH抵押品的价值在用户打算在这种协议的稳定货币中铸造的价值的135%到150%之间(“抵押比率”)。 这些稳定货币尚未偿还，但当ETH价格下跌时，用户抵押品的价值低于协议的抵押品比率，用户抵押品自动清算，ETH出售以封闭用户借来的稳定货币。 所有这些都是自动和自主发生的，确保协议的抵押品永远不会低于未补偿稳定货币的价值。

考虑到过度担保的稳定货币在严重动荡时期取得了成功，这种可编程的安全机制应该受到赞扬，不应该停止。

监管算法稳定货币

FSB认识到算法和数字资产的重要作用，因此有很好的机会为算法稳定货币推荐适当定制的监管框架。
但目前起草的提案几乎明确要求有效禁止算法稳定货币中选择所需的族。 建议限制使用加密货币作为储备，并指出稳定货币不应该“从算法中获得价值”，因为所有稳定货币通常需要在维护资产和高流动性资产上获得1:1的支持。

更仔细的定制要求可以更好地保护区块链生态系统和用户。 FSB应开展研究，分析超额抵押稳定货币的相对安全性，以评估哪些抵押品和抵押品的比率可能足以允许继续使用此类抵押品。 例如，一项监管建议可能切实建议，只有市值超过某一值的数字资产才能作为抵押品，使作恶者无法轻易操纵抵押品资产。
此外，125%以上的抵押率在最近的变动中被证明有效，值得进一步研究。

另一方面，广泛禁止算法稳定货币可能损害国际金融体系。 首先，稳定货币在中心化货币政策失败的国家提供了稳定性，无论是托管还是算法。
越来越多的国家面临着日益增大的通货膨胀我预计稳定货币的使用会增加。 此外，算法不仅对稳定货币发展至关重要，在区块链生态系统的其他方面也很重要，如DeFi和其他数字资产市场。 如果监管机构将算法视为不稳定的来源，web3开发人员认为这是对他们项目的威胁，可能会退出市场。
如果有适当的规定，我们可以防止这个结果。

简而言之，关于算法稳定货币的高级原则是

禁止算法稳定货币，只是盲目同化所有算法稳定货币，实际上是非常不同的。
稳定货币带来的系统风险是担保设计的产物，而不是算法的使用。
禁止所有算法稳定货币就像用锤子敲碎坚果一样。

算法禁止稳定货币会扰乱目前的DeFi市场，导致很多客户的损失。 从投资者保护和软件开发的角度看，禁令具有破坏性和适得其反，可能给政策制定者试图保护的用户造成数十亿美元的损失。

禁令将对DeFi和更广泛的整个web3行业产生意外的负面影响。
算法稳定货币协议中使用的算法机制普遍存在于DeFi和web3中。 区块链生态系统可能会将全面禁止算法稳定货币视为对这些机制的攻击，这可能会无意中阻碍广泛的web3创新。

禁令极其难以执行。 由于选择实施FSB批准禁令的各全球司法管辖区无法从市场上移除所有算法稳定货币，禁令可能鼓励监管套利，使用户面临更大的伤害风险。

禁令将创新强加于监管框架特别宽松的地区，损害了监管良好的大型发达经济区块。 禁令可能会加速发达国家web3开发者市场份额的下降，阻碍web3和影响更广泛行业发展的能力。

不需要禁令。 因为其他限制措施会更有效地降低系统风险。 监管机构可以利用现有监管规定，防止近期大部分系统性损害，新的准确监管规定可以消除此类系统性损害再次发生的风险，而不会阻碍创新。

总结

监管机构和政策领导者深思熟虑地监管区块链技术至关重要。
感谢有机会对这些重要事项发表评论，因为它们逐渐成为金融体系的重要支柱。 我们将这封评论信视为公共部门和私营企业之间持续对话的一部分，并期待着继续就这些问题进行接触。 根据

央行等发布的《关于进一步防范和处置虚拟货币交易炒作风险的通知》，正文内容仅用于信息共享、不对任何经营和投资行为进行推广和背书，请读者严格遵守所在地区的法律法规，不参与任何违法金融行为。 不为虚拟货币、数字收藏类发行、交易和融资等提供交易入口、指引、发行渠道引导等。


原文链接

注意律动模块Beats、中银保监会等五部门2018年8月发布的《关于防范以「虚拟货币」「区块链」名义进行非法集资的风险提示》文件显示，请公众广泛理性看待区块链，不要盲目相信花哨的承诺树立正确货币观念和投资理念，切实增强风险意识对发现的违法犯罪线索，可以积极向有关部门举报和反映。