[xy001] leveragefromnftcollectionleveragev3by Michael n [xy 002] [xy001]执笔： MIDDLE.X

审稿： Owen编辑： Eunicen原文标题及链接：继Shuming hao123 @ QQ.com [xy 002] [xy 001] steem事件后，今年年初，货币圈话题孙宇晨(Justin Sun)再次陷入了关于统治攻击的指控。 作为拥有超过10亿美元加密资产的巨鲸Tron公链的创始人，孙宇晨的链上地址受到加密侦探们的广泛追踪。

gfxlabs报道，2022年1月，据链上记录，孙宇晨疑似住所向AAVE借入大量$MKR，并在社区内提议建立DAI-TUSD交易对支持两者按固定1:1汇率兑换。 这一行为引起注意后，受到社区的抵制，这个地址最终没有用这些$MKR开始提案，而是直接归还。 三月，另一个疑似属于孙宇晨的地址从Compound借入大量$COMP，价值约1300万美元，充值货币贬值，很快新地址收到货币贬值约900万美元的$COMP该地址以这些$COMP发起提案，提议在Compound中添加TUSD作为抵押资产，该提案最终在社区广泛参与的投票中被否决。

尽管所有操作都以失败告终但是，该事件在业界引起了对DeFi对策的讨论。 有些人认为，鲸鱼利用“纸币能力”，直接影响治理决策是不能接受的，德夫的治理也不应成为金钱政治。 也有怀疑孙晨宇住所的行为完全按照治理规则进行，而且巨鲸们用自己的财务资源争夺在迪夫I的资产准入资格，有助于提高治理许可价格，而治理许可价格的提高反过来又有助于促进更多人和更多资金的参与。 为什么高兴？

持后一种观点的人以Curve协议流动性激励机制的成功为主要论据。 作为以稳定货币为焦点的AMM交易市场、Curve创造了向不同交易对的流动性提供者提供不同力量$CRV报酬的流动性激励方式，奖励力度依赖于治理投票中各交易对获得的投票比例。 该机制引发了各稳定货币项目方在治理投票中的激烈竞争被称为“Curve War”。
许多稳定货币项目方将用尽全身解数，获得更多投票权，获得更多流动性。 [xy 002] [xy001]从2020年开始，Curve协议就一直在实施这种流动性激励政策这给Curve协议带来了巨大的成功。 通过诱发Curve War，推动了$CRV的价格上涨，$CRV的价格上涨刺激了更多资金为Curve协议提供流动性流动性的增加进一步加剧了Curve War，完美的飞轮效果！ [xy 002] [xy001]没有人认为curve的统治被金钱政治绑架了但是，Curve War上出现了寻找规则漏洞的天才项目。 Mochi Protocol

可能是受到了Curve War的飞轮效应的启发Mochi Protocol也打算开启属于自己的飞轮效果。 Mochi Protocol使用其治理令牌$MOCHI INU来刺激USDM稳定硬币在Curve中的流动性，利用其拥有的大量$MOCHI

INU凭空铸造了大量的USDM。 然后，Mochi Protocol将这些USDM替换为DAI，在DAI上大量购买$CVX (拥有大量CRV投票权的Convex Protocol的治理通证)进一步争夺流动性，继续利用这些流动性将USDM更换为DAI，购买$CVX循环往复。
USDM流动性达到1亿美元时，Mochi Protocol开始覆盖行驶通道，耗尽池内流动性，禁用USDM挂钩，完成流动性提供者收割。

使用

*cvx在Convest上投票可以间接影响Convest保险箱的veCRV投票，从而简化了该过程。 *

到此为止关于DeFi治理中的金钱和政治态度可能有矛盾。
它一方面可能给协议带来成功，另一方面也可能暴露治理攻击和鲸鱼操作的风险。
如果不改变观点，我们就很难摆脱对金钱政治的直觉阐明DeFi治理中的真正问题。

DeFi治理中的真正问题

Paka Labs是目前的DeFi治理机制之一，治理杠杆

鲸鱼参与治理本身是无可非议的。 问题是孙宇晨住所用于参与治理的$COMP和$MKR涉嫌来源于贷款而不是长期持有的资产。 如果这个地址添加到合同中的是某种高控盘资产，他完全有可能通过“印钞”，将协议作为他的ATM，他几乎不需要承担$COMP或$MKR的价格下跌风险。 这不符合激励兼容性原则。 这个地址通过去中心化的贷款协议借了管理通行证，还得自己提供抵押品，实际上如果借款主体没有足够的抵押资产，也可以通过发行债券衍生品向他人借款管理通行证。 [xy002] [xy001]在curve war中存在大量收购Curve War的参战项目们用少量奖励激励其他有投票权的人按照他们的意愿投票。
当然，这里的“一点点”是针对他们直接购买这些投票权。 贿选还包括通过经济激励方式让别人委托自己门票，因为Curve的管理没有委托机制，所以这种行为在Curve War中没有出现。（xy002 ）） xy001)利用门票和贿赂来治理参与者们，使他们能够获得的投票权及其必要的责任不成比例。

此外，很多DeFi协议，如果治理参与率过低，投票权比例极低，就可以决定重要资金和资源相关的重要事项，是天然的杠杆。 例如6月19日，Solend只使用了几十万美元的投票权于是，决定接收某条巨鲸的亿美元资产，令人咋舌。
这个决议受到社区的强烈反对，在新的提案中被废除了。

总之，治理投票中存在金融杠杆，这是真正威胁治理公平和安全的重要问题。

其二，无人看守

DeFi的管理比其他类型的道的管理更为复杂。 因为DeFi拥有的资源不仅仅是协议Treasure的资金也不是TVL的资金，实际上TVL资金的所有权不属于DeFi合同本身，这也是Solend接手巨大的鲸鱼账户引起巨大争议的原因。
对于DeFi合同来说，最重要的资源往往是非财务资源。 例如，

-贷款合同中担保资产白名单

- DEX中的流动性资源

是通过治理投票来分配合同的非财务资源的具有一定的资源销售性质。
从这个角度来看，Curve War可以理解为Curve对自身流动性资源的拍卖行为。
既然不是政治，就与金钱的政治无关。（治理通证承担着分配有价资源的权力，这就是Compound官方宣布$COMP没有财务价值后，价格依然疯狂的原因，聪明的钱们早就意识到了这一点！（xy002））xy001
)真正导致风险的环节是没有人审查资产准入。
比较一下中心化交易所的货币投放流程。
Web3项目在中心化交易所投放货币往往需要支付货币投放费用。
此外，中心化交易所还将对项目进行后台调查。 如果积压失败，则不会陈列令牌。
负责的交易所不会采用“有钱就能进”的货币政策吧。
但是，许多DeFi协议没有对资产准入设立任何风控审查措施。
这样的类比并不完全合适，但可以说明一定的问题。

社区成员可以主动注意治理建议，但像Compound和MakerDAO驳回孙宇晨地址疑似建议一样，他们会动员更多成员通过投反对票来驳回添加恶意资产的建议但是这种社区成员的自愿监管责任主体不足，专业能力也不足，不是结实的网，总是“漏网之鱼”趁虚而入。 例如，2月15日对Build Finance的治理攻击提案在社区没有注意到的情况下被攻击者控制的少数选票静静地通过。
这次攻击使协议金库的资产几乎为零，使Build Finance全面失败，难以翻身。
为了保障

defi参与者的资金安全需要更严格的资产准入审查机制。

如何消除治理杠杆？

需要逐一解读使用治理杠杆的手段。

防御借出单：在锁仓交换统治权

首先、借票行为比较容易防御，基于时间加权和基于声誉的投票可以降低借票的影响。 事实上，Curve的治理已经采用了基于时间加权的投票。 Curve的统治权力通过使用veCRVveCRV必须通过锁定CRV获得，而不是通过CRV投票获得。
锁定期间越长，veCRV的获得量就越多。 例如，锁定期间4年可以获得1 veCRV，锁定期间1年只能获得0.25 veCRV。

这里有两个关键点。 其中之一是veCRV不能汇款。 在Curve War中，用户可以将veCRV借给Convex、StakeDAO或Yearn Finance因为Curve为少数主体打开了白名单； 其二，随着锁定的$CRV接近过期日期，veCRV的数量将线性减少，需要持续更新锁定时间以保持投票权。

锁头机制使得任何人都无法通过短期贷款获得大量投票权。
想要获得更多的投票权，就必须延长贷款时间，这样会给租房者增加很大的成本。

我们认为，未来主要的DeFi协议很可能演化为类似Curve的时间加权机制，或者更复杂的声誉投票机制，越来越多的新协议也倾向于不再采用简陋的1T1V机制。

选择防御贿赂：选择隐私技术或成为希望的

贿赂行为比较难防御。

行贿虽然存在于现实政治中，但不是气候。 无记名投票的特点是投票者向投票箱扔选票后第三方不能知道投票者投了哪个选项，甚至投票者本人也很难拿出可靠的证据证明给投票者投了某个选项，对收藏交易缺乏可靠的基础。 在

链中，收藏行为的信息较高对收藏者来说很容易验证，但涉及收藏行为的主体身份信息却难以隐藏，难以追究责任。 这是打造收藏市场几乎完美的土壤。 在Curve War上，贿选已经成为参战项目的常客，为此，专门的收藏服务平台应运而生，通过这些平台，可以将令牌奖励与用户的选票进行交换。 [xy 002] [xy001]积木协议更公开地宣称要打造通用的收藏平台打着“帮助戴奥提高统治参与率”、“帮助统治通证持有人挖掘统治价值”的旗号，意在在DeFi统治的语境下，“收购”一词成为中性词。 确实，贿选可以提高治理参与率但是，DeFi协定想看到的肯定不是这种虚假的高参与率。

理论上，协议可以主动屏蔽收藏平台的投票，剥夺收藏投票权，但这是基于收藏平台的信息公开，如果收藏平台运行在专用服务器上，或者是在区块链上利用隐私技术开发的，没有办法主动屏蔽。。 《DAO 的另一面：链上贿选和黑暗 DAO 的崛起》的文章阐述了利用TEE硬件构建隐秘并购交易平台的可行性方法。

是否可以构建看不见投票信息的治理系统？ 例如，使用隐私技术，单个用户的投票信息在链上变得不可见，并且从外部只能看到可验证的最终投票结果，而且投票的用户可以是可信的，以证明他们对哪个选项投了票或者委托了谁。
这提供了一个抛砖引玉的思路，希望行业伙伴一起探讨、一起探索。

需要注意的是，即使是最完美的技术也不能完全杜绝收藏。
例如，依靠熟人关系的收藏交易是无法阻止的。 我们能做的就是防止收购选择形成有效的市场，以免DeFi治理被一般的收购行为完全异化。

提高治理参与率：治理政党与治理激励

在DeFi行业的一些基准协议中也有也可能没有很高的治理参与率。
例如，Compound的治理参与率只有5%左右。
有些人认为这是通过掌握投票权从共识中获益的动力。 低投票率意味着一些协议将被多层间接管理，以实现更大的杠杆化，有关详细信息，请参阅操作Fei-Index-Aave中的诸神。

从实践民主的角度来看，人们总是试图让更多的人参加投票，但从协商统治的安全性来看，目标应该是投更多的票给统治。
如果你改变目标，我们可以找到新的统治构想——协商政党。

尽管一些协议已经开发了移动民主机制，人们仍可以将治理通行证委托给他人间接参与治理。 但是，该机制受制于几个因素，无法大幅提高治理参与率。

-除非深入参与社区，知道谁是活跃的贡献者，知道其治理投票倾向，否则不知道委托谁投选票合适

-受委托投票者的活跃度积极参加几次投票可能就再也没有投过票了，但委托人似乎总是不关注是否应该更改委托。 因此，一些选票长期陷入沉默。

-大多数协议没有为参与治理提供报酬因此，货币持有者希望将管理通行证放入DeFi生存。

引入具有特定投票倾向的联盟可以改善上述情况。
我们可以把它称为“协商政党”。 政党向选民承诺负责任地参加投票以获得投票然后，政党雇佣专家，仔细研究所有决定，协商实现这一点。

当然，为了让协商政党负责任地参与治理，并且持卡人有动力将票委托给协商政党，协商必须对治理参与者给予充分的激励。

治理激励的存在相当于对不参与治理的人征税，有助于唤醒沉默的选票。 治理激励分为两部分，一部分是为锁仓治理通证发放的奖励，类似于PoS公链中的Staking奖励，另一部分是对投票行为的奖励例如，投票次数达到多少可以获得奖励，这部分奖励可以补助金的形式给予执政党。
激励的来源可以是增发通货膨胀，也可以是协议利润。

这里需要注意。 协商政党不能再发行自己的统治通证了否则，就会给Fei-Index-Aave这样的伊娃型杠杆化带来机会。 即使协商政党颁发了治理通行证，也应该任命专门的委员会来决定投票，而不是直接由自己的治理投票来决定投票。

目前，WildFireDAO已成立为协商政党，积极参与多项协议的管理。
Rabbithole也成立了自己的管理委员会，参加自己持有的协议的管理投票。
期待协商政党未来的进化！

如何设定门卫的结构？ [xy 002] [xy001
]发生mochi治理攻击后，Curve通过治理取消了Mochi Protocol的竞争流动性资格，但与事后的“资产清算”相比，我们需要提前的资产准入环节，防范欺诈行为，更好地保障缉毒参与者的资金安全。

如上所述，在许多DeFi现行的资产准入机制中，只要有足够的钱，就可以获得足够的投票权然后，将想要添加的资产放入DeFi中。 作为贷款合同的抵押品、作为稳定货币的储备资产或被允许加入特定交易对，从而释放治理攻击的风险。 通过消除治理杠杆，这可以增加攻击者获得投票权的成本，但除此之外，DeFi协议还需要门卫机制作为防止添加恶意资产的最终安全屏障。

让很多货币持有者审查资产准入是不合适的否则，回到最初的问题，投票权可能被攻击者短期捕获而实施治理攻击，不能进行全体投票者对资产负责的背景调查。 可能的办法是，投票者们制定审查标准，任命风控小组回退资产然后，决定是否释放。

标准制定后，必须注意审核委员会无权释放不符合标准的资产或阻止添加符合标准的资产。 否则，协议可通过治理投票罢免或更改委员会成员。
当然评审标准只是几个字，在实践中一定有评审委员会的自由裁量权。 但考核标准应尽量明确(例如，一项资产去中心化程度可以用一个尺度来衡量)，减少考核委员舞弊、受贿的可能性。 这就像现实政治中的立法和司法的分离。

实际上，Compound，SushiSwap有一个类似“元老院”的结构，“元老院”有权否决所有治理提案，即使是高票通过的治理提案。
实践中、“元老院”也负责资产准入审查，负责驳回新增恶意资产的提案。

但是，这个机制也在讨论中。 支持者认为元老院的权力和治理投票的权力可以相互平衡，实现民主政治中两院制那样的结构，反对者认为可以否决所有提案的元老院，完全有可能成为协议的独裁者。

我认为这其中的核心有两个。

-元老院的权力范围，除了提案否决权以外是否还有其他权力，在一些治理结构中、元老院还有暂停协议、启动紧急提案等权限，在一些发展初期的DeFi协议中，元老院有可以随时更新协议代码的超级权限。
的权限范围决定了元老院的性质——独裁者还是守门员。 但是，对于发展比较初期的DeFi，由于代码尚未成熟，经济体系也尚未验证，以独裁者为守门员也是无奈之举

-元老院成员的选举和罢免，是否由治理投票决定这决定了元老院是独立存在的权力实体还是只是治理投票站的权限代理机构？

总之，我们认为应该由管理投票授权和监督的委员会负责资产审查。
该委员会可以是独立的部门，也可以由协议的“元老院”兼任。

总结[xy 002] [xy 001]随着defi的发展，一些协议已经成为Web3的基础设施，具备公共物品属性，保护参与者的资金安全，是defi发展的基础。 风险因素主要存在于两个方面、一是治理权力向金融杠杆放大，可能导致权责不均衡等治理，二是缺乏可靠的资产准入审查程序(门卫机制)，对诈骗者也要拒之门外，有钱可以在DeFi协议中增加任何资产

本文给出了消除治理杠杆的几种方法，在这些方法中，用仓锁机制防御借据已经得到广泛应用，用治理政党和治理激励提高治理参与率也相继实践，只有收藏还是个棘手的问题存在过高的技术门槛，并不是短期内就能实现的。 此外，本文还提出了设置门卫机制，根据既定原则委托风控团队对添加到DeFi许可证的资产进行调查和审计。 但是，在DeFi的统治实践中为了解决上述问题，可能会有更好的方法。
DeFi的管理将走向何方，我们会继续关注并研究。