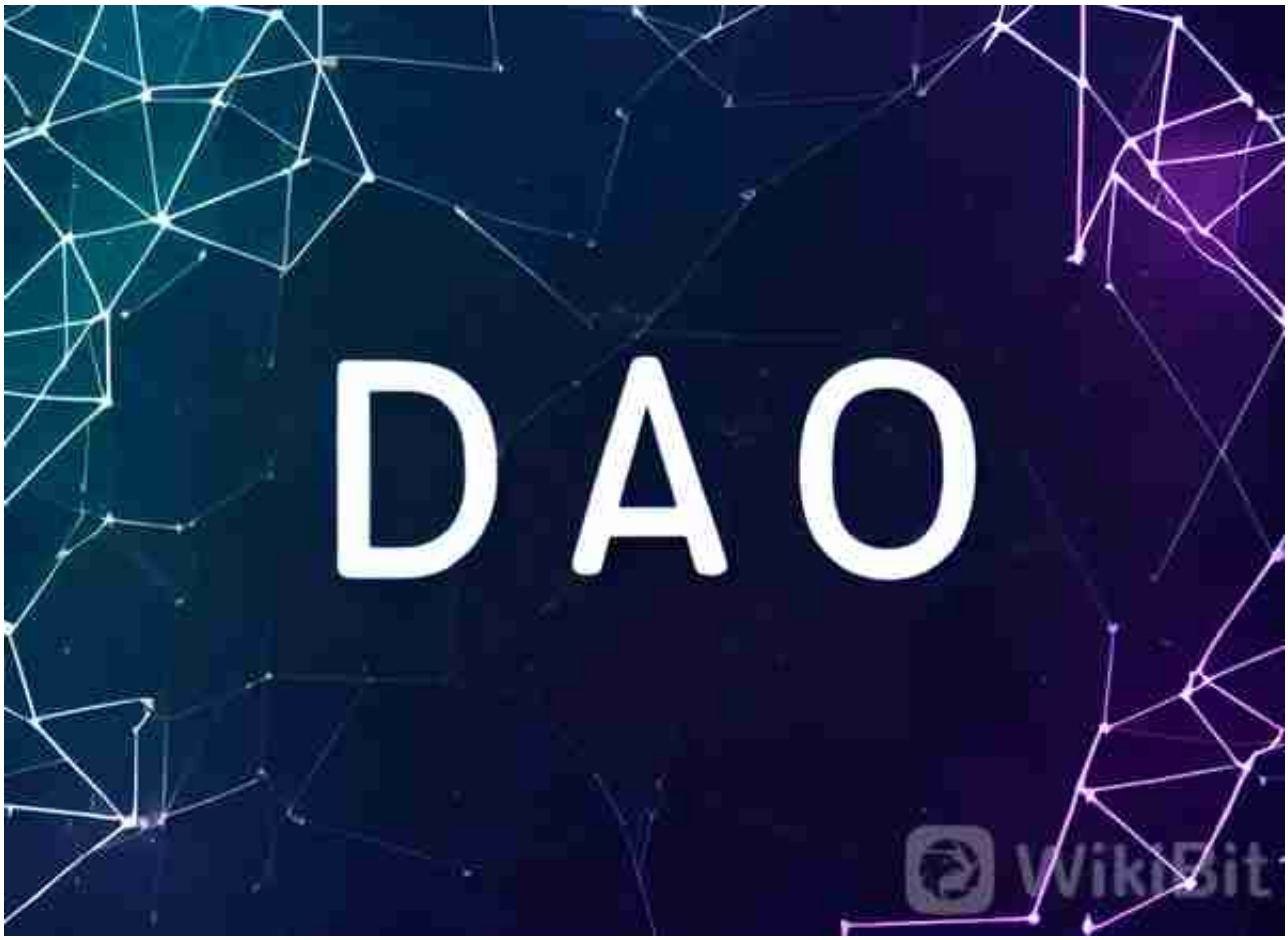


TLDR
:治理风险可能来自很多领域，社会、经济或技术风险——可以是三者的组合。
构建未来的治理体系，了解如何降低风险是建设未来的关键。
最重要的是，并不是所有的事情都需要投票！

去中心化合同具有永久性。 合同的变更都是通过管理的治理流程进行的。
统治过程本质上是人参与的，所以要复杂得多。

本文探讨治理过程中的一些危险，为思考治理风险提供一个通用的框架。 总体而言，有效的治理过程旨在防止作出将项目或合同朝着与特派团不同的方向推进的决策。

这里概述了三个主要的风险类别：技术、社会和经济。
此外，还有有效治理进程中的一些重要经验和教训。

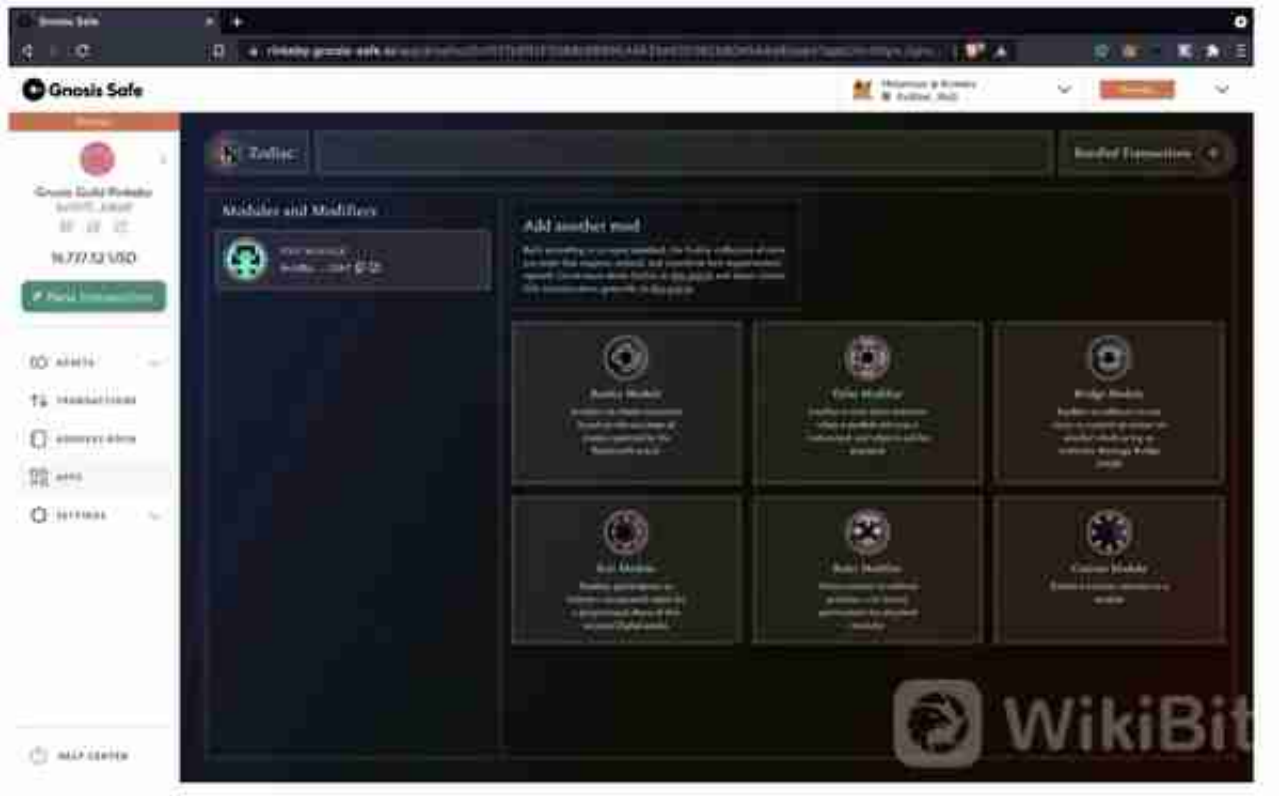
最小化治理的过程

最小化治理行为的治理系统更加稳健和可维护。 变化越少越好。
但是，协议需要升级。

广泛的治理体系还涉及许多非共识性问题，例如是否承诺提供资金这可以说是重要的决定，但不会从根本上影响共识。
能够区分特定协议选择和社会层面选择的系统减少了治理行为的总体范围。

自治组织本来就是自治，减少它们的统治足迹可以降低对人的依赖。

正如我们所说，许多工具正在开发中，旨在帮助对社会或人际协调的治理行为和影响协议的行为采取不同的方法。 例如Zodiac
Module的出现，以便用户提交交易并乐观地进行验证。
在所有链条上行动不需要投票，只有在交易提出，交易性质有分歧时才需要投票。



安全多重验证的Zodiac模块

技术漏洞

智能协议漏洞是许多协议的棘手问题，包括治理协议许多治理契约作为一种链上投票机制存在，执行一组指定的指令。 只要链中有代码，就可能出现技术漏洞。

此类风险的明显例子是2200万美元的Compound治理漏洞。
Compound系统负责流动性开采奖励分配的合同有缺陷。

唯一有权更改受影响合同的合同是总督合同，这意味着只有治理投票才能影响纠正错误合同更改。

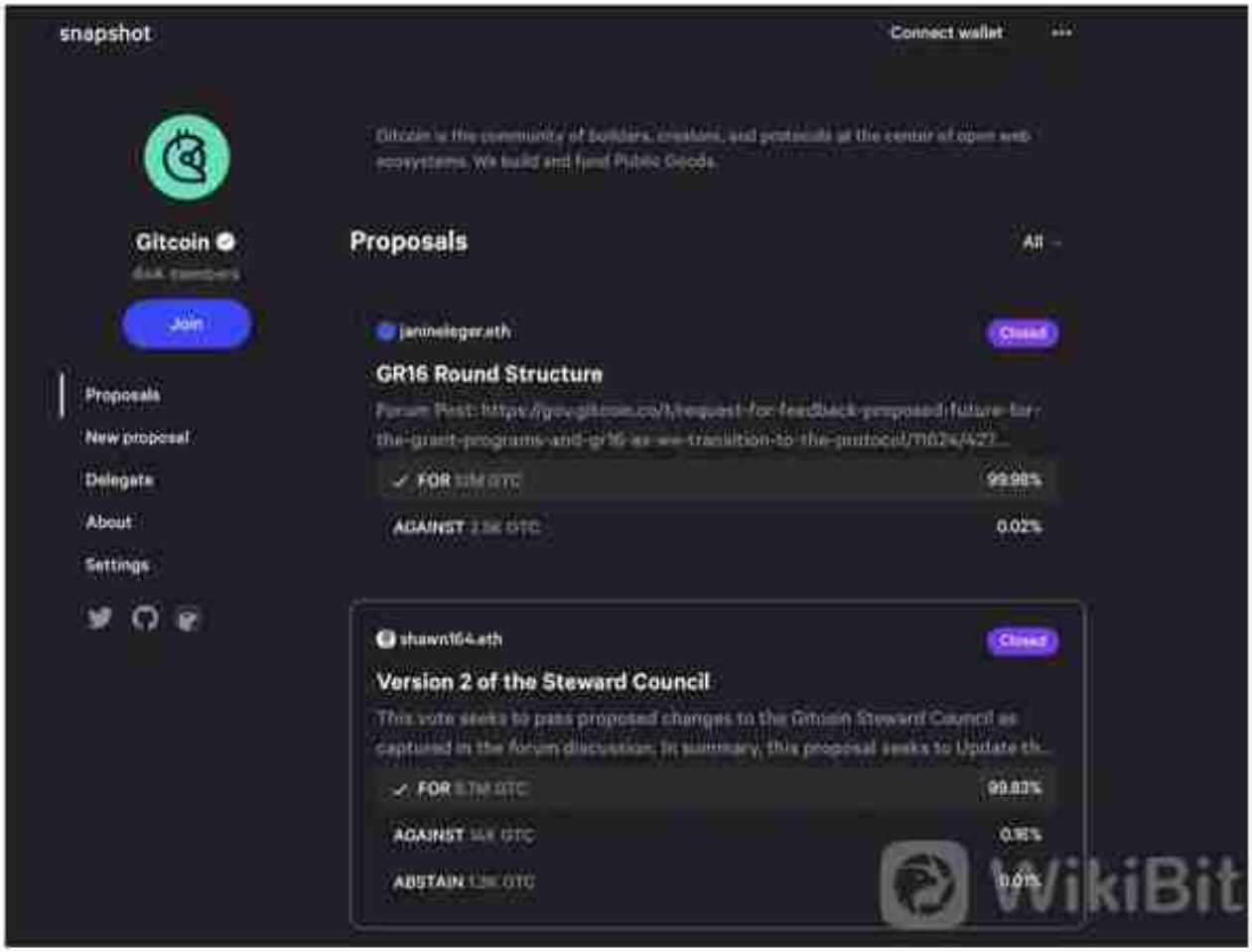
缓慢的管理流程阻碍了漏洞的修复和资金流动的阻止。
幸运的是，对于Compound团队来说，响应尽可能快，治理系统也尽可能快。

从另一个角度看，合同完全按照规则执行，包括漏洞。
只是，人类认为合同的目的和实际合同的代码不一致。

不管我们每个人的想法是对是错，实际上，人类认为用代码能做什么和它意味着什么总是有区别的。 令人惊讶的是，我们总是直到很晚才意识到这一点。

社会脆弱性

不仅在技术方面，在治理的社会方面也有自己的挑战。 人类当然比代码复杂。



快照：链下投票工具

链上vs链下投票：如上所述，协议治理行为应该最小化到绝对基础。
链上投票应该影响链上合同，链下投票被指定为人们社会上可以达成共识的项目。
我经常看到通过在几百个链条上投票可以很容易地达成软协议。
与标准运营项目相比，这自然会降低重要投票的重要性。

投票的机制和流程。
并不是所有的投票过程都遵循这一趋势，但有足够的方法值得警惕。
在某些情况下，对链外的“温度”检查会导致链上的投票，由多个签名者执行。

作为从链条上投票的步骤是没有意义的。 放弃链上的部分，是否有可靠的多重签名管理软件共识让连锁投票采取必要的行动吗？

统治过程中最有价值的项目是合格选民的注意力，更多的选票会降低选民的冷漠和长期投票率。
只有确认声音有意义，提出要点，达到全面投票的水平，才能确保投票结果。

法定人数和所需参与人数：正如上一篇文章所写，在选民参与和组织规模方面存在着权衡。
但是，在权力下放和少数创始团队成员轻易推翻投票的能力之间也存在权衡。
如果令牌没有足够分散一个团队可以满足投票法定人数的要求。

选民专业知识：最高的治理风险之一是选民做出明智选择所需的专业知识水平。 多数情况下，用户有资格廉价地获得管理令牌(空投、清算开采流程等)并进行投票。
选民不知道投票内容是什么，要么弃权，要么根据别人的倾向做出最受欢迎的决定。 这不会导致充分的中心化和代表性投票。

经济脆弱性

经济利用意味着攻击者可以引入资金来接管投票过程。
大多数情况下，治理通过可购买的令牌进行。 这意味着获得投票份额(例如51%)的成本。

从理论数字来看，国库必须至少拥有其他合同50%的投票供应价值才能完成这一利用。
因为有的国库规模比其他国库大几个数量级，所以这种类型的风险范围并不牵强。

幸运的是，许多协议锁定了足够数量的令牌，流通供应不足，这样的攻击是现实的。
但是，有了这个令牌，经济攻击可以解锁时间表，并随着时间的推移循环供应。

随着时间的推移，这种攻击可能不经济。
也许是为了打败竞争对手，影响有争议的投票，造成僵局而获得控制权。

在鲜为人知的协议中，可以看到基于经济攻击的协议使用案例： True Seignorage。 xy 002 xy001
tldr版本是，因为他们的市值足够小，攻击购买了他们51%的投票令牌。
获得令牌后，攻击者开始投票，并在其地址铸造11.5 quintillion令牌。
投票自然而然地通过了用户可以在Pancake swap上卖尽可能多的令牌。

攻击者从令牌销售中获得的利润超过了通过投票的成本，但Dev钱包没有足够的资金阻止他。

结语

治理将继续存在，我们有责任建立将我们推向我们希望进入的未来的治理进程。

了解治理体系的风险以及如何应对这些风险是一个发展过程。
一个明显的趋势是治理系统有缺陷履行诺言需要深思熟虑。

去中心化管理还处于起步阶段，其背后的技术也是如此。
随着行业的成熟，治理攻击的向量自然消失。