A Call for a Temporary Moratorium on "The DAO"

暂时停止 DAO 的呼吁书

DRAFT (v0.3)
草案（V0.3）

作者：Dino Mark, Vlad Zamfir, Emin Gün Sirer
dino at smartwallet dot org, vlad@ethereum.org, egs@cs.cornell.edu
May 26, 2016
(revised May 29, 2016，修改)

翻译： Kang Xie

Over the past 3 weeks a Distributed Autonomous Organization (DAO) known simply as 'The DAO' and implemented as a smart contract on the Ethereum blockchain, has raised 11.5 million Ether, valued at $150 million at the time of writing. This is the largest crowd-funding event in history. The DAO now controls 16% of the total supply of Ether. It is arguably the most visible project in the Ethereum ecosystem.

在过去短短的三个星期，DAO（去中心化的自主组织）在以太坊的区块链上实施了智能合约，并且融资了 1 千 1 百五十万的以太币，价值大约在$1.5 亿美元左右。这是史上最大的一次众筹活动。DAO 现在已经控制了全世界 16%的以太币供应。它已经是以太坊生态圈里最引人注目的一个项目。

In this paper, we analyze the rules of The DAO and identify problems with its mechanism design that incentivize investors to behave strategically; that is, at odds with truthfully voting to reveal their preferences. We then outline potential attacks against The DAO made possible by these behaviors.

在这篇呼吁书里，我们会分析 DAO 然后指出它设计上的一些问题。它们可以激励投资者不会真实地投票来反映他们心中的选择，因为这样做对他们战略上有利。我们还将列出这些可以让他们发起对 DAO 的几种攻击的行为。

In particular, we identify nine causes for concern that can lead DAO participants to engage in strategic rather than honest behaviors. Some of these behaviors can cause honest DAO investors to have their investments hijacked or committed to proposals against their interest and intent.

具体来讲，我们会指出九个战略上考量可以让 DAO 的参与者的行为变得政治化而不是诚实地参与投票。这些政治化的行为会危及到其他诚实参与者的利益，比如说绑架他们的投资或是对伤害他们利益和意图的建议做出承诺。

We discuss these attacks, and provide concrete and simple suggestions that will mitigate the attacks, or in some cases make them completely impossible.

我们会讨论这些攻击，然后提供实际和简单的建议来降低这些攻击的危害或是让这些攻击变得无效。

We would like to call for a moratorium on proposals to prevent losses to the DAO caused by unintended consequences of its mechanism design. A moratorium would give The DAO time to make security upgrades, and should be lifted only once the DAO is updated.

我们还想呼吁暂时停止 DAO 的融资行为以防因为它设计上的缺陷而造成损失。一个暂时中止可以让 DAO 更新它的安全系统，然后在更新后被取消。

Introduction（介绍）

Smart contracts enable the collection and disbursement of funds according to immutable computer programs. Built on a Turing-complete platform, such contracts have the capacity to create constrained and predictable financial constructs without a trusted entity. Distributed autonomous organizations are one such class of contracts that can carry out corporate functions in accordance with the will of their shareholders, while being constrained by programmatic bylaws. These programmatic bylaws, if written with sufficient care can obviate the need for a management team in certain constrained domains.

智能合约使得用电脑程序来融资和发放资金变得可能。这些合同建立在图灵完备的平台之上然后可以在没有一个信托机构的情况下建立有约束力和可预测的金融架构。分布型自主组织（DAO）就是这类合同的一员，它可以根据股权持有人的意愿来执行公共决策。这些可被编程的规则如果想得周全的话，可以在一些特定限制的领域里替代一个职业管理团队。

Perhaps one of the most suitable such domains is crowd-funding. In traditional crowd-funding, a corporation such as Kickstarter connects investors with individuals or organizations who propose ventures. When the proposal gathers sufficient opt-in from the investors, it can proceed. If it succeeds, it returns financial rewards to its investors. The crowd-funding platform extracts some overhead for the matchmaking service it provides in the middle.

或许其中最有可能的一个领域就是众筹。在传统的众筹里，一个企业比如像 Kickstarter 把投资方和提出创业建议的创业者或是创业组织撮合起来。当这个建议得到投资方足够的支持的时候，它就可以运作。如果它成功了，它就可以向投资人回报利润。然后这个众筹平台在此过程中收取一定的运作费用作为它当红娘的服务费。

Another potential domain is investment funds or venture capital firms. In traditional venture capital firms, the managers collect funds from investors, evaluate proposals for various ventures, and determine a subset of ventures to fund. Successful ventures bring returns to the fund, from which the fund managers extract some, often substantial, overhead for the decision-making service they provide in the middle.

另外一个可能的领域就是投资基金或是风险投资公司。在传统的风投公司，这些管理员从投资者那里融资，评估不同创业建议的风险，然后从中选取一部份建议来投资。成功的创业投资可以带来回报，然后管理员从中提取为数不少的费用作为他们从中做出决定的服务费用。

Over the last month, we witnessed the emergence of a distributed autonomous organization, known as The DAO, that is a cross between these two domains and seeks to completely eliminate the middlemen. The DAO operates somewhat like a venture capital firm, in that it collects a pool of funds to invest in worthy proposals, but it differs in that all the individual investors are able to vote, in proportion to the size of their investment, on each investment proposal put forward to the fund. The aspirational goals for The DAO are to utilize the wisdom of the crowds for this decision-making process, and to eliminate the risks posed by middlemen using a programmatic approach to corporate management.

在上个月，我们见证了一个分布型自主组织的崛起，它叫做 DAO。它是两个领域的混合体然后想要完全地消除中间人。DAO 的运作像一个风投公司，因为它融资来投资给一些有价值的创业建议。但它又不同因为每个投资人都可以对每个放在桌面上的投资建议来按照他的投资份额来投票，DAO 的梦想是一方面利用众人的智慧来决策，另一方面用自动程序的方法来替代人工管理来消除中间人可能犯的错误。

The DAO is unique in many ways. It was funded through a crowd-funding effort that quickly raised 11.6M ether (worth approximately $150M at the time of writing), making it the largest crowd-funded project in history. At this funding level, The DAO commands approximately 15% of the total ether in existence. Because The DAO is so large, and because it is one of the first smart contracts of its kind, it has garnered much attention. Consequently, public opinion about decentralized autonomous organizations rides on its success.

DAO 在许多地方是独一无二的。它以惊人的速度用众筹的方法迅速地融资 1 千 1 百 6 十万以太币（价值现在大约在 1.5 亿美元），这个记录使它成为史上最大的一个众筹。在现在这个融资高度上，DAO 大约掌握了 15%所有存在的以太币。因为 DAO 是如此庞大，也因为它是它这个种类的第一个智能合约，所以它吸引了许多注意力。这样一来，公众对未来智能合约的信心与意见就建立在它的成功与失败之上。

Yet smart contracts pose unique technical challenges. Recall that computer programs can and most often do contain bugs. When a desktop application has a bug, it may crash; when a smart contract has a bug, it may render funds irrecoverable. Moreover, the smart contract cannot be easily updated, unlike desktop apps and other traditional software. Thus, careful thought and considerations must be put into constructing a smart contract that carries out the intended operations of a complex decision-making investment fund, especially in the presence of potentially malicious participants.

虽然智能合约有着独一无二的技术上的挑战。因为电脑程序经常有 bug。当一个桌上应用有 bug，它会崩溃。但是当一个智能合约有 bug 的时候，它可能让投资荡然无存。甚者，智能合约不能够轻易地被更新，不像一般的电脑应用和软件。所以，在建立一个智能合约的时候，我们更要对其复杂的决策过程进行严密的考量，尤其在有潜在恶意的参与者的时候。

In this paper, we focus specifically on The DAO and examine the operational details of The DAO's smart contract with an emphasis on its mechanism design. We then identify nine causes for concern, where the mechanisms encoded into the current implementation of The DAO can give rise to unwanted strategic behaviors for the participants that are at odds with the primary function of the organization. In the case of The DAO, we show that in the current implementation can attacks with severe consequences are possible. We identify an attack that can indefinitely tie up investor funds and lead to ransom demands; an attack that enables a large cartel to usurp funds; and another attack that can enable an attacker to depress the value of the native fund tokens, among others.

在这篇论文里，我们着重于 DAO 和检查它智能合约执行的细节，我们的重点在于它的算法设计。我们指出九个令人担忧的理由，当这个算法被写进 DAO 现在的实施之后，它会制造一些我们不希望看到的投资者的政治行为会与这个组织的主要理念背道相驰。在这个案列里，我们会证明对于现在的实施方案的攻击可能会造成严重的后果。我们会指出其中一个攻击可以无限期地绑架投资者的资金从而导致赎金的要求；另一个攻击可以让一个卡特尔篡夺资金；还有一个攻击可以打压 DAO 筹码的价值；还有其他一些攻击。

At a fundamental level, these attacks all stem from unintended consequences of the mechanisms built into The DAO. Some are facilitated by an inherent bias towards voting to fund proposals; the current system discourages people from voting when they perceive a proposal to have negative expected value. A second fundamental problem stems from the structure of the withdrawal process: investors wanting to exit from the fund by "splitting" are vulnerable to attack. Combined, these problems can give rise to complex strategic behaviors, all resulting in a corruption of the intended, honest debate and voting process to select the most deserving proposals.

在本质上，所有这些攻击都是由于 DAO 里面的一些算法所造成一些没有估计的后果所造成的。有些是由一个对投资建议投票的内在偏见所造成的。现在的系统不鼓励投票，如果他们收到一个提议是有负面期望值的。第二个基本问题源自取款的过程架构：投资者通过"分裂"的方法如果他们想要退出基金的话，但这个方法易于被攻击。综合起来，这些问题导致了一些复杂的政治行为，然后就会腐蚀原本诚实的讨论投票来选择最有价值的投资建议的过程。

In the rest of this paper, we describe the operation of The DAO, the voting bias, potential attacks, and then discuss some potential mitigations and solutions. The central take-away from our analysis and discussion is that it would be prudent to call for a temporary moratorium on whitelisting proposals so that reasonable measures can be taken to improve the mechanisms of The DAO. Therefore, we call on the curators to put a moratorium in effect.

在余下的篇幅里，我们会描述 DAO 的具体运作，投票倾向性，可能发生的攻击，然后讨论一些可能的缓解或是解决方法。我们主要目的是想通过我们的分析和讨论让大家意识到现在暂时停止 DAO 的白名单建议是一个审慎的做法，这样一来就可以改善 DAO 的内部运作。所以，我们呼吁 DAO 的监护者马上进行暂时搁置。

There are two alternatives to a curator-imposed moratorium. One is to ask The DAO token holders to place a self-imposed moratorium by voting down every proposal with overwhelming majority. Due to the flaws involving negative votes outlined in this paper, it would be a mistake to depend on this mechanism to protect against attacks targeting the same mechanism. The second alternative is to ask the DAO token

holders to opt-in to the security measures by holding a vote for a new curator set who will implement a moratorium. We believe that The DAO's default behavior should favor security. Since no one knows the percentage of non-voting, non-active token holders, the threshold required for curator changes may be too high for the voting process to meet. For these reasons, we believe that the safest and most immediate course of action would be for the curators impose a moratorium, and allow the DAO token holders opt-out by means of a curator change vote.

除此方法之外，还有其他两个替代选择。第一是要求 DAO 的筹码持有人自动执行暂时搁置，用绝对多数的选票把所有的投资建议打压下去。由于这篇论文所列出的反对票的设计缺陷，想依靠反对票的程序来防止对反对票程序的攻击会是个错误。第二个选择是 DAO 的筹码持有者可以通过投票选举一组会执行暂停的新的监护人班子来选择安全措施。因为没人知道弃权者和不活跃的筹码持有人的比例，所以要想达到换掉监护者班子的投票临界值可能会很高。所以，我们认为最直接有效的方法就是监护人马上叫暂停，然后让 DAO 的筹码持有人可以通过换监护人班子的投票来反对这个决定。

The Structure of The DAO

DAO 的结构

The primary function of The DAO is to serve as a crowd-funding investment vehicle. To this end, The DAO API is structured around an initial creation phase that collects funds and an operational phase which consists of collecting proposals, voting on them, optionally funding them, and performing administrative functions such as paying out rewards and withdrawing funds. In the following discussion, we cover the operation of the DAO in each of these phases, and discuss the main abstractions behind the DAO to provide a context for game-theoretic analysis of the operation of this smart contract.

DAO 的主要功能是成为一个众筹投资的载体。为了达到这个目的，DAO API 的结构主要围绕着两个阶段：第一阶段是起初融资阶段和一个营运阶段包括了搜集投资建议，投票选举，有选择地投资，然后执行行政功能比如像付出奖励和取出资金。在下面的讨论里，我们会讨论每个阶段里 DAO 的运作，然后讨论 DAO 后面主要的提象化概念来提供一个用博弈理论来分析智能合约的理论框架。

The DAO was created on April 30, 2016 at 10:00 UTC, based on a specific instantiation of The DAO contract. This paper describes the operation of this smart contract.

DAO 在 2016 年 4 月 30 日格林威治时间 10：00 诞生，是由 DAO 合同的一个特别的实例化。

Creation and Funding Phase

创始和融资阶段

The DAO creation phase started with the initial creation of the smart contract and lasted for 27 days. During this period, The DAO issues tokens, called The DAO Tokens (TDT), in exchange for Ether sent to a designated funding address.

DAO 的创始阶段开始于一个智能合约起初的创立然后会延续 27 天。在这段时间里，DAO 会发行筹码，叫做 DAO 筹码（TDT），用来兑换发送到一个指定融资地址的以太币。

The buy-in price of TDT varies during the creation phase. First, it starts at 1.00 ether for 100 TDT for the first 14 days. Then, there is an increase of 0.05 ether per 100 TDT for the following 10 days, then a final 3 day period at 1.50 ether per 100 TDT.

在这个创始阶段，TDT 的购入价格不断在改变。刚开始的 14 天内，1 个以太币换 100TDT。然后的十天里，增幅为每 100TDT 0.05 个以太币，最后三天里，每 1.5 个以太币换 100 个 TDT。

Late investors who paid more than 1.00 ether per 100 TDT have their surplus ether above 1.00 placed in a special account called extraBalance. Individual token holders cannot withdraw their funds from the extraBalance account; this money can only be moved after an amount equal to the extraBalance has been spent on proposals. In effect, the extraBalance represents additional money made available to the fund for spending on proposals, money earned by the DAO through additional fees paid by late joiners. For example, if a token holder paid 1.05 Ether for 100 TDT, and if no Ether had been committed to any proposals, the token holder could still only withdraw 1.00 Ether. The extra 0.05 Ether will stay locked in until The DAO has funded proposals that, in aggregate, exceed the amount of the extraBalance. Only then is the extraBalance folded into the main balance of the DAO, where it is distributed proportionally to TDT holders. At the time of writing the extraBalance is approximately 275,000 Ether.

后进的投资者如果每买 100TDT 多付 1 个以太币，这些多付的币会放在一个特殊的账号叫做多余存额。个人的筹码持有者不能够从这个账号里提取资金；这笔币只有在相同数目的币被用在投资提议之后，才可以动用。事实上，多余存额代表了额外可以投资在提议上的币值，也就是 DAO 的后来加入者所付的额外费用。举例说，如果一个筹码持有者付了 1.05 个以太币来买 100TDT。这额外的 0.05 个以太币会被锁住直到 DAO 投资提议的总额超过了多余存额的总额。直到那个时候，多余存额才会被纳入 DAO 的总额，然后它会被按照比例分配给 TDT 的持有人。在写本文的时候，多余存额里大约有 275，000 个以太币。

The DAO follows a pattern where the main contract acts as a factory for sub-contracts that split off from the main DAO. In what follows, we will refer to the initial contract simply as The DAO, its children as child-DAOs, and collectively to any contract that implements the 'Standard DAO Framework' as a DAO. The process of generating child-DAOs can continue recursively, until a depth limit is reached.

DAO 按照一定流程来制造合同。主合约就像是副合约的干细胞工厂，副合约从主合约上分裂出来。按照这个逻辑，我们称原始合约为 DAO，它的衍生合约为子 DAO。然后把那些实施“标准 DAO 框架”的任何合约通称为 DAO。繁衍子 DAO 的过程可以反复进行下去，直到一定的深度。

The Curator

监护者

Every instance of The DAO has a designated curator that is responsible for adding addresses to and removing addresses from the proposal payment address whitelist. The 'Curator' account for the current instance of The DAO is a 5 out of 11 multi-signature address (note that one of the curators has announced that they will not participate, although his key technically still has the right to sign in the multisig).

每个 DAO 的实例都有一个指定的监护者来负责从提议支付地址的白名单里添加删除地址。在现在这个 DAO 的实例里的这个监护者账号是一个 5-of-11 的多个签名地址（请注意其中有一个监护者宣布他不会参加，虽然他的钥匙在技术上依然可以签署这个多个签名）。

Only addresses on the whitelist can submit proposals to, and be funded, by The DAO. Proposals that want funding from the DAO must to ask the curator to add their address to the whitelist. Thus, the curator ensures that some human supervision is involved in the selection of proposals to be funded for the DAO. In effort to shield curators from legal liability, their responsibilities are limited strictly to deterring "malicious proposals." The main motivation for the curator abstraction is a majority takeover attack where a large (53%) voting bloc votes to commit 100% of The DAO's funds to a proposal that benefits solely that bloc. The curator concept was introduced mainly to weed out such proposals and either refuse to whitelist their payment addresses or to un-whitelist their addresses; curators are expected not to take profitability or business sense into account while making whitelisting decisions. The task of exercising business judgment over the proposals is left up to the wisdom of the crowds through the proposal and voting process.

只有在白名单上的地址，才可以提交建议和得到 DAO 的投资。如果提议想得到 DAO 的投资的话，他们必须向监护者请求把他们的地址加入白名单。因而，监护者保证了在选择可以得到 DAO 投资的建议的时候有人为监控。为了保护监护者不会有法律上的麻烦，他们的责任严格地限制在阻止有恶意的提议。监护者这个提象概念的建立的主要动机是防止一个多数掌管的攻击，在这个攻击里一个 53%的投票派系投票把 100%的 DAO 的币投给只对他们有利的一些提议。所以监护者的概念被引入主要是把这些提议过滤掉，然后不拒绝把他们的地址放入白名单也不会把他们地址从白名单上除去。当他们在做白名单的决定的时候，他们不因该从商业赚钱的角度考虑这个问题。对这些提案商业上的考量完全取决于投资者的智慧和选举结果。

Proposals and Voting

提案和投票选举

Once a proposal has its address whitelisted by the curator, token holders can then vote on whether or not they want to fund that proposal. All TDT holders are allowed to vote either YES or NO, and their votes are weighted by the amount of their TDT holdings. The voting commences for a minimum voting period of 14 days, at the end of which the weighted votes are tallied. A simple majority of YES votes is required for a proposal to be successfully funded, and a minimum quorum of voters is required in order for the voting phase to be closed. The minimum quorum varies between 20 to 53% depending on the size of the proposal. Very large proposals will require a 53% quorum, while small ones only need 20%. There is no limit to how many proposals can be simultaneously going through the voting process. In order to prevent proposal spam, there is a non-refundable listing fee for each proposal.

一旦一个提案的地址被监护者放进白名单，筹码持有者就可以投票选举他们是否愿意投资那个提案。所有的 TDT 持有者都被允许选择是与否，然后他们的投票按照他们 TDT 的持有量被加重。一个投票过程最少 14 天，在最后被加重的票数会被统计出来。一个简单的大多数“是”可以让一个提案成功地得到投资。此外要达到一个最少投票人的数额才可以结束投票过程。最少投票人的数额比例大约在 20%和 53%之间随着提案的大小变化。非常大的提案要求 53%的最少投票人比例，小的大约只要 20%左右。对于同时对有多少提案可以进行投票选举没有定额。为了防止垃圾提案，每个提案都有一个一次性的登记费。

Voting is an activity that limits future actions available to a TDT holder. Critically, if a token holder votes either yes or no on a proposal, they cannot change their vote, nor can they withdraw from the DAO through a split until the voting period has ended, nor can they transfer their TDT. Voting on any proposal places a TDT holder on a list of ‘blocked’ addresses that cannot perform splits or transfers. For a TDT holder who votes on multiple proposals, the block remains in effect until the latest of the voting deadlines. If the proposal on which a TDT holder voted succeeds, the holder can only withdraw their share of the Ether balance that is left after the winning proposal has been funded.

投票是限制一个 TDT 持有者未来行动的一个措施。重要的是，如果一个筹码持有者对一个提议投赞成或是反对票，他们不能改变他们的投票，也不能在投票周期结束之后通过一个分裂来从 DAO 里面退出。一个 TDT 的持有者，只要他在任何提议上投了票，他就会上了一个“被锁住”的地址名单阻止他进行分裂或是转账。如果一个 TDT 持有者在几个提议上都投了票，这个锁住会一直持续到最后一个投票的截止期。如果 TDT 持有者所投票的提议成功了，持有者只能够在中标的提议等到资助之后，才能提取在以太余额账户里属于他们的份子币。

In contrast, token holders that do not vote can withdraw from the DAO by initiating a split. Splits take 7 days to fork off the funds; consequently, a split initiated by a user 7 days ahead of a proposal’s voting deadline can operate without any risk that her funds will be spent on that proposal.

相反，没有投票的筹码持有人可以通过一个分裂从 DAO 里提身出来。分裂需要 7 天时间才能够从基金里分叉出来。因此，如果用户在提议投票截止期的前 7 天时间里发启一个分裂，它的币就没有被用在那个提议上的风险。

Splitting and Withdrawals

分裂和提币

The DAO does not permit funds to be withdrawn as Ether directly. Instead, token holders can take their TDT out by a process known as a ‘split’, a process that takes 34 days in total to complete and involves creating a new DAO.

DAO 不允许用以太币直接地提币。相反，筹码持有者可以通过一个“分裂”来提取他们的 TDT，这个过程大约需要 34 天左右来完成和制造新的 DAO。

The split process begins by having a token holder initiate a special proposal with a new curator address and a funding amount of 0 ether. The voting period on a split proposal lasts a minimum of 7 days. The outcome of the vote on a split proposal is inconsequential, as the proposal cannot be executed. Instead, the presence of a split proposal whose voting period has ended confers the right to split from The DAO to the parties who voted YES on it. This takes place when these parties call a function called 'splitDAO' to move their funds from The DAO into a newly formed child-DAO contract. This provides a way to withdraw one's funds from The DAO; namely, individuals who wish to withdraw from The DAO initiate a new curator proposal, where they themselves are the new curator, wait for the voting period to expire, and then transfer their holdings to a newly created DAO.

这个分裂过程起始于一个筹码持有者发起一个特殊的提议，这个提议有一个新的监护人地址和 0 个以太币。一个分裂建议的投票期为 7 天。这个投票的结构不重要，因为这个提议不会被执行。相反，这个已经结束投票的分裂提议把可以从 DAO 分裂出来的权限交割给那些投赞成票的人。技术上说，这些投票人会启动一个功能叫做 '分裂 DAO' 把他们的资金从 DAO 的母体里剥离出来放进一个新产生的子 DAO 合约。这提供了一个让人从 DAO 里提取资金的方法；其实，这个过程就是那些想从 DAO 提取资金的人启动一个新的监护人提议，把自己作为监护人，等待投票期过期，然后把他们的资金转到一个新建立的 DAO。

When a token holder splits from The DAO through the above mechanism, the usual 27-day creation period for a new DAO still applies. This means that the whole process takes 34 days in total to initiate a split proposal (day 0), gather votes (for 7 days), split from The DAO, and then wait for the new DAO to be formed (for 27 days). The actual transfer takes place on the 7th day and the funds are tied down for 27 days. When a token holder has successfully split into their own new DAO, they can create a proposal to pay themselves out the full balance of all the Ether left in the new DAO.

当一个筹码持有者用上述的方法从 DAO 里脱离出来的时间是 7 天，制造新的 DAO 通常需要 27 天，两个加起来意味着整个过程需要 37 天左右，从启动一个分裂提议（0 天），搜集投票（要 7 天），从 DAO 里分裂，然后等待新的 DAO 产生（27 天）。真正的转账在第 7 天发生，然后资金被锁住 27 天。当一个筹码持有者成功地 "分裂" 进入他们自己的 DAO，他们就可以自己提出一个提议来把这个新 DAO 账户里面所有的以太币转给自己。

Transferability of TDT

TDT 的可转性

TDTs that are not blocked due to voting are fully transferrable to any valid Ethereum address, and therefore can be sold immediately on exchanges or over the counter. Thus, if a token holder does not want to wait 34 days to split from The DAO and withdraw their ether, they can just sell their TDT tokens directly on exchanges for ether, or perhaps even other cryptocurrencies such as Bitcoin.

没有被投票锁住的 TDT 可以完全转给任何一个有效的以太地址， 然后马上就可以在交易所里卖掉。所以，如果一个筹码持有者如果不想等上 34 天后从 DAO 里分裂出来然后提取他们的以太币，他们可以在交易所上直接卖掉他们 TDT 来换取以太币，或是其他币种比如比特币。

Attacks and Concerns

攻击和忧虑

Analyzing an investment vehicle such as The DAO is difficult. This is partly because game theoretic treatments typically require a full characterization of the actors, the potential moves available to them within the game, and the various payoffs associated as a result of each move. In an interconnected financial system involving convertible assets with a large number of complex actors, there are many potential payoffs, not all of which can be expressed within the narrow confines of a game. That is, not all actors try to maximize their returns in ether, and instead may have exogenous payoffs in dollar terms that are difficult to capture. For instance, an actor who has purchased put options on ether and damages the system's reputation via an attack on The DAO may well lose tokens in the game but come out ahead financially, and modeling their profit requires quantifying social factors and market effects. Many previous attempts to apply game theory to distributed systems or complex agent systems have suffered from simple-minded modeling that has, at times, led to incorrect conclusions. Consequently, we do not attempt to provide a full game theoretic treatment of The DAO in this paper. Instead, we discuss the guiding principles for good mechanism design that ought to apply to crowd-funding investment vehicles such as The DAO, and identify several weaknesses in the current structure of The DAO that violate these principles and open the shareholders to attack.

分析一个投资工具比如像以太坊是困难的。部分原因是用博弈理论通常需要对每个角色进行角色分析，他们可能走的每一步，还有每一步所造成的盈利结果。在一个互相连接有许多可转化的资产和许多复杂角色的金融系统里，有很多盈利的方法，但所有这些因素是无法用一个博弈理论的狭隘理论框架来表达的。道理是，不是所有角色是用以太币来最大化他们的利润的，相反，有些的利益最大化是用美元的外源利润来体现的。举例说，一个角色买了以太的看跌期权然后发动一个攻击来损害了系统的声誉，虽然他在 DAO 里面损失了 TDT，但依然最后得利。想要对他们的盈利模式建模需要量化社会因素和市场影响。许多以前尝试用博弈理论来分析复杂的分布性系统最后都失败，因为他们的建模想法太简单，最后导致错误的结论。所以我们也不想在这里用博弈理论来分析 DAO。我们只是想讨论适用于众筹投资工具内部运作设计的一些指导原则，然后指出在现在 DAO 架构里的一些弱点违反了这些原则，让投资者会受到攻击。

Guiding Principles

指导原则

The central point of the DAO is to enable token holders to vote on proposals. A rational actor will cast her vote in a manner that is informed by the net present value she perceives for each proposal. Every proposal has a clear present cost, specified in the proposal itself. It returns value to the shareholders either through an expected profit denominated in ether and paid back to The DAO, or through the implicit appreciation of the TDTs. As with every investment, proposals to the DAO have a probability of success that depends on the nature of the venture and its business plan. For instance, a proposal may ask for 1000 Ether to make 1000 T-Shirts, and may estimate that they will sell 1000 T-Shirts at a profit of 5 Ether each over a time frame, and thus estimate they will return 5000 Ether to The DAO. It is expected that vigorous debate and discussion during the voting phase will enable each voter to independently estimate the chances of success, and thus, the expected value (EV).

DAO 的中心思想是让筹码持有者可以投票选举提议。一个理性的角色是会根据她所收到的每个提议的净现值来投票。每个提案都有一个现在成本，在提议里被清楚地列出。然后它会向股份持有者返利，要么通过一个用以太标价的预期利润付还给 DAO，要么通过 TDT 的一个潜在升值来达到。就像每个投资机会，向 DAO 提交的投资案成功几率取决于它的本质和商业计划书。举例说，一个投资提案想要融资 1000 个以太币来印 1000 件 T-shirt，预测经过一定的时间每件 T-shirt 可以获利 5 个以太币，所以他们估计可以向 DAO 返回 5000 个以太币。可以期望的是在投票过程中的激烈讨论和辩论会让每个投票人独立地估算成功的几率，也就是期望值（EV）。

A DAO is considered to have good mechanism design if actors incentivized to vote truthfully in accordance with their estimates of the expected value of each proposal. For the wisdom of the crowd to manifest itself, we would like a TDT holder to vote YES for a proposal that they believe has positive expected value (+EV), and NO for a proposal they believe has a negative expected value (-EV); alternatively, they may abstain if their vote is not going to change the outcome. We now describe why the current implementation of The DAO fails to uphold this principle.

一个良好的内部运作设计可以激励 DAO 里的角色真实地按照他们对每个提案的期望值来投票。为了激发集体智慧，我们期望 TDT 的持有者投赞成票如果他们觉得这个提议有正的期望值（+EV），否定票如果他们对这个提议的期望值是负的（-EV）；另外，他们可以弃权如果他们的投票不能改变结果。我们现在就来描述为什么现在实施的 DAO 没有遵守这个原则。

The Affirmative Bias, and the Disincentive to Vote No

表示赞成的倾向性和妨碍投反对票

The current DAO has a strong positive bias to vote YES on proposals and to suppress NO votes as a side-effect of the way in which it restricts users' options after they vote. Specifically, the current DAO blocks token holders from splitting from the DAO or from selling their TDT once they have voted on a proposal, until the voting period ends. Thus, a voter who believes a proposal has a negative expected value is in a quandary: they can split from The DAO immediately without taking any risk, or else they can vote NO and hope that the proposal fails to be funded. A NO vote is therefore inherently risky for an investor who perceives the proposal to be -EV, in a way that voting YES is not for a +EV voter. As a consequence, The DAO voting is likely to exhibit a bias: YES votes will arrive throughout the voting period, while a strategic token holder will want to cast their NO vote only when they have some assurance that the outcome of the vote will be NO. Strategic NO voters will cast their votes only after gaining information on others' negative perception of the same proposal, so the voting process itself will not yield reliably signal information about the token holders' preferences over the course of the voting period. Preferences of the positive voters will be visible early on, but the negative sentiment will be suppressed during the voting process -- this can result in an affirmative bias that can be a problem for a crowd-funding organization where YES results in funding projects.

现在的 DAO 有个很强的倾向性来投赞同票然后压制反对票，这是由于它限制用户投票后的选择所造成的一个不良后果。具体地说，现在的 DAO 阻止筹码持有者在他们对于提议投票之后从 DAO 分裂出去，或是卖掉他们的 TDT。他们一直要等到投票期结束。因此一个投票者相信一个提议有负的期望值的时候会处于一个困境: 他们要么可以马上毫无风险地从 DAO 分裂出来，或是他们可以投反对票然后希望这个提议不被通过然后再获得退款。

这样一来投反对票对一个期望值是负的投资人来说是有固有风险的。而投赞成票对于一个期望值是正的投票人来说则不一样。这样一来，DAO 的投票过程就会表现出这种倾向性：在整个投票过程中，赞成票会不断地进来，而想投反对票的人只会在他们可以确定投票结果是反对的情况下才会投票。有计谋的反对票者会先搜集其他人对这个提议的反面印象的情报后才会投下反对票，所以这个投票过程本身就不会对筹码持有者的真正趋向产生可靠的信息。投赞成票人的趋向会很早就显现出来，而投反对票的趋向会在整个投票过程被压制 – 这就造成一个众筹组织的问题 - 表示赞成的倾向性会导致最后的赞成来资助项目提议。

The Stalking Attack
“跟踪”攻击

Splitting from The DAO (the only existing method of extracting one’s Ether holdings from the main DAO contract) is currently open to a “stalking attack.” Recall that a user who splits from The DAO initiates a new DAO contract in which they are initially the sole investor and curator. The intent is that a user can extract his funds by whitelisting a proposal to pay himself the entire contents of this contract, voting on it with 100% support, and then extracting the funds by executing the approved proposal.

从 DAO 里分裂出来（从现在来说这是唯一可以从主要 DAO 合同里提取以太币持有财产的方法）会暴露在“跟踪”攻击之下。我们上面说过一个从 DAO 分裂出来的用户启动一个新的 DAO 合同，在这个合同里他既是唯一的投资者又是监护者。这样做的意图是这个用户可以通过这个方法取出资金: 先把一个提议放进” 白名单”里，然后把这个合同里的所有基金支付给自己，投 100%的赞成票，然后执行这个被批准的提议来提取资金。

However the split and the resulting sub-contract creation takes place on a public blockchain. Consequently, an attacker can pursue a targeted individual by buying tokens during the creation phase. Since a splitting user is the new curator of the nascent sub-contract, a stalker cannot actually steal funds; the victim can refuse to whitelist proposals by the stalker (though note that, due to potential for confusion and human error, the expected outcome from such attacks is still positive). If the stalker commits funds that correspond to 53% or more of the sub-contract, he can effectively block the victim from withdrawing their funds out of the contract back into ether. Subsequent attempts by the victim to split from the sub-contract (to create a sub-sub-contract) can be followed in the same manner, trapping the victim’s funds and prohibiting conversion back to ether. The attacker places no funds at risk, because she can split from the child-DAO at any time before the depth limit is reached. This creates the possibility for ransom and blackmail.

但是这个分裂和接下来产生的的副合同的创立是在公共的区块链上发生的。所以，一个攻击者可以跟踪一个被盯上的用户。跟踪者在副合同的创立阶段买筹码。因为一个分裂出来的用户是刚刚产生副合同的新的监护者，一个跟踪者不能真正地偷币；因为受害者可以拒绝把跟踪者的提议放在白名单之上（我们还是要注意到，因为有混乱和人为的错误，这种攻击的结果还是有可能得策的）。如果这个跟踪者投入相当于整个副合同的 53%或是更多资金的话，他可以有效地阻挡受害者从副合同里把 TDT 提出来换成以太。之后受害人想要从副合同里分裂出去的尝试（创立副副合同）就可以用同样的方法来阻止，从而锁住受害人的资金和制止它转换成以太币。这个攻击者则不会损失任何资金， 因为她可以在

任何时候在深度限制达到之前从子 DAO 里分裂出来。这就为绑架勒索要赎金制造了可能性。

An initial response to this problem suggested some remedies for preventing and counterattacking during a stalker attack. These remedies not only require unusual technical sophistication and diligence on behalf of the token holders, but are technically insufficient to deter stalking. The suggested prevention technique is to never split with a proposal on which any other party has voted YES. This is insufficient because an attacker can programmatically vote YES on every split with a dust account to earn the option to split, and then transfer his funds before invoking split. Once a victim finds herself in a child-DAO, Slockit has suggested two counterattacks for the victim to try to fend off the attacker. Neither of them are resilient against an attacker that creates dust accounts to vote, then transfers the money to the dust account that voted for the grandchild-DAO that the victim decided to pursue. These strategies are not guaranteed to win (they rely on launching trap and ambush attacks against the attacker), withdrawals are not a constant time (and gas) operation, and much more importantly, not only do these counterattacks require immense technical sophistication, they would severely impact the user experience and overall user satisfaction.

对于这个问题起初有人建议了一些弥补措施来防止和回击这类攻击。但这些措施不仅要求有不同寻常的技术复杂性和筹码持有人本身的努力之外，它还是不足以阻遏攻击。这个提出的防御措施是永远不从一个别人已经都赞成票的提议上分裂出去。但这个措施是不够的，因为一个攻击者可以用程序和一个粉尘账户对每个分裂投赞成票来获取分裂的选择，然后在引发分裂前把资金转走。当一个受害者在一个子 DAO 里，Slockit 曾经建议过用两个反击战术来抵抗攻击者。但是这两个方法都缺少灵活性：当攻击者制造一个粉尘攻击账户来投票，然后把币转入这个粉尘账号来攻击那个受害人想要执行的孙子 DAO。这些战略并不一定能够成功（他们的成功取决于对于攻击者的发起圈套和埋伏攻击），提款不是一个恒定的时间与燃料的运作，更加重要的是，不仅仅是这些反攻击手段需要很高的技术程度，它们会严重地影响到用户体验和总体的满意度。

The Ambush Attack

埋伏攻击

In an ambush, a large investor takes advantage of the bias for DAO users to avoid voting NO by adding a large percent of YES votes at the last minute to fund a self-serving proposal. Recall that under the current DAO structure, a rational actor who believes a proposal is -EV is likely to refrain from voting, since doing so would restrict his ability to split his funds in the case that the proposal succeeds. This is especially true when the investor observes that sufficiently many NO votes already exist to reject the proposal. Consequently, even proposals that provide absurdly low returns to The DAO may garner NO votes that are barely sufficient to defeat them.

在一个埋伏攻击里，一个大的投资人利用 DAO 用户避免投反对票的倾向性在最后一分钟里投许多赞成票来资助一个对自己有利的提议。还记得在现在的 DAO 结构下，一个理性的角色如果相信一个提议是-EV 的，他不会主动投票，因为主动投票会限制他从 DAO 里分裂出来的能力万一这个提议最后成功的话。这个情况尤其明显如果这个投资者观察到有足够多的反对票来否决这个提议。结果是，即使是那些对 DAO 收益很低的提议，DAO 也不能收集到足够的反对票来否决它们。

This kind of behavior opens the door to potential attack: A sufficiently large voting bloc can take advantage of this reticence by voting YES at the last possible moment to fund the proposal. Such attacks are very difficult to detect and defend against because they leave little to no time for The DAO token holders to withdraw their funds. Among the current DAO investors, there is already a whale who invested 888,888 Ether. This investor currently commands 7.7% of all outstanding votes in The DAO. For a proposal that requires only a 20% quorum, this investor already has 77% of the required YES votes to pass the proposal, and just needs to conspire with 2.3% of the token holders, in return for paying the conspirators out from the stolen funds.

这种行为会为可能的攻击打开大门： 一个足够大的投票集团可以利用这种集体沉默在最后投赞成票来通过提议。这种攻击很难被发觉和防御因为它不会给 DAO 筹码持有者留下足够多的时间来提取资金。在现在的 DAO 投资人里，已经有一个大腕投资了 888，888 个以太币。这个投资者现在掌控 7.7%在 DAO 里所有的表决控制权。

The Token-Value Attack

筹码价值攻击

In a token-value attack, a large investor stands to benefit by driving TDTs lower in value, either to profit from such price motion directly (e.g. via shorts of put options), or to purchase TDTs back in the open market in order to acquire a larger share of The DAO. A Token-Value attack is most successful if the attacker can (i) incentivize a large portion of token holders not to split, but instead sell their TDT directly on exchanges, and (ii) incentivize a large portion of the public not to purchase TDT on exchanges. An attacker can achieve (i) by implementing the stalker attack on anyone who splits and then making that attack public on social media. Worse, since the existence of the stalker attack is now well-known, the attacker need not attack any real entity, but can instead create fictitious entities who post stories of being stalked in order to sow panic among The DAO investors.

在一个筹码价值攻击里，一个大的投资者可以打压 TDT 的价值，要么从这个价值下滑里直接套利（比如说做空一个看跌期权），或者是在公开市场里买回 TDT 来获得 DAO 里的更大份额。一个攻击者的筹码价值攻击被认为是最为成功如果他做到以下两点：i）激励大部分的筹码持有者不分裂，而是在交易所上直接卖掉他们的 TDT。ii）激励大部分的公众不在交易所里买 TDT。一个攻击者可以通过以下的办法来做到 i）对于任何分裂出来的人进行跟踪攻击，然后在社交媒体上把攻击公布出来。更糟糕的是，如果这个跟踪者攻击的存在是广为人知的，这个攻击者甚至不需要攻击任何真人，只需要制造一些假身份然后开始散布谣言他被攻击了，从而在 DAO 的投资者里制造恐慌。

An attacker can achieve (ii) by creating a self-serving proposal widely understood to be -EV, waiting for the 6th day before voting ends, and then voting YES on it with a large block of votes. This action has the effect of discouraging rational market actors from buying TDT tokens because (a) if the attackers proposal succeeds they will lose their money, and (b) they don’t have enough time to buy TDTs on an exchange and convert them back into Ether before the attackers proposal ends, thus eliminating any chance of risk-free arbitrage profits. The combined result of (i) and (ii) means that there will be net selling pressure on TDT, leading to lower prices. The attacker can then buy up cheap TDT on exchanges for a risk free profit, because he is the only TDT buyer who has no risk if the attacking proposal actually manages to pass.

一个攻击者可以通过以下方法达到（ii）：制造一个为自己谋利但是大多数人都认为是-EV 的提议，然后等到在投票选举结束前的第 6 天，然后用众数票投赞成票让它通过。这个战术可以让有理性的市场参与者不买 TDT 筹码因为（a）如果攻击者的提议成功他们会丢币（b）他们没有足够的时间在攻击者提议结束之前在交易所里买 TDT 然后把它们换成以太币，因而消除了任何没有风险的套利的盈利机会。（i）和（ii）的综合结果意味着 TDT 上有净出售压力，从而导致更低的价格。这个攻击者因此可以在交易所里买到廉价的 TDT 来获得没有风险的利润，因为他是唯一的没有风险的 TDT 买家如果他的攻击提议得到通过。

The extraBalance Attack

额外余额攻击

In the extraBalance Attack, an attacker tries to scare token holders into splitting from The DAO so that book value of TDT increases. The book value of TDT increases because token holders who split can not recover any extraBalance, so as more holders split, the extraBalance becomes a larger percentage of the total balance, thus increasing the book value of the TDT. This attack is made more severe by the fact that once an amount equal to the value of the extraBalance has been spent, a proposal can be created to send any amount of eth to extraBalance and the curator is not able to prevent this via the whitelist.

在一个额外余额攻击里，一个攻击者想要恐吓筹码持有者从 DAO 里分裂出来来升高 TDT 的账面价值。TDT 的账面价值升高因为筹码持有者分裂出来后不能拿回任何的额外余额，所以越多的筹码持有者分裂，额外余额会占总余额里越大的比例，从而升高 TDT 的账户价值。这个攻击可以变得更加严重一旦一个与额外余额一样大小的币量被使用后，可以建立一个提议把任何量的以太币打给额外余额账户而监护者没有办法通过白名单来制止这个行为。

Currently the extraBalance is 275,000 Ether, which means the book value of TDT should be 1.02. If the Attacker can scare away half the token holders, the TDT will increase in value to 1.04. If the Attacker can scare away ~95% of the token holders, the book value of the remaining TDT will be roughly 2.00. In this attack, the Attacking Whale would do the opposite of the token-value attack by creating a self-serving proposal with a negative return and then immediately voting YES on it with a large of TDT, thus scaring all the token holders, and then giving them 14 days until the end of the voting period so that they have more than enough time to safely split. In this scenario, splitting will be risk free (assuming that it is not coupled with a stalking attack), since voting NO could result in losses if the attackers end up having enough YES votes.

现在额外余额里有 275，000 个以太币，这意味着 TDT 的账面价值是 1.02. 如果这个攻击者可以把一半的筹码持有者吓跑的话，TDT 的账面价值会增加到 1.04. 如果这个攻击者可以吓跑 95%的持有者的话，TDT 会增加到 2.00。在这个攻击里，这个攻击大腕会发动与筹码价值攻击相反的攻击：先建立一个让自己得利的-EV 的提议然后用一个大的 TDT 集团投票来迅速投赞成票，从而把所有的筹码持有者吓跑，然后给他们 14 天时间一直到投票期结束这样他们就有足够时间来安全地分裂。在这个情况下，分裂是没有风险的（假设它没有和一个跟踪攻击挂钩起来），因为投反对票会导致损失如果这个攻击者最后没有拿到足够的赞成票。

The Split Majority Takeover Attack

分裂大多数接管攻击

Even though the DAO white paper specifically identifies the majority takeover attack and introduces the concept of curators to deter it, it is not clear that the deterrence mechanism is sufficient. Recall that in the majority takeover attack outlined in the DAO whitepaper, a large voting bloc, of size 53% or more, votes to award 100% of the funds to a proposal that benefits solely that bloc. Curators are expected to detect such instances by tracking identities of the beneficiaries. Yet it is not clear how a curator can detect such an attack if the voting bloc, made up of a cartel of multiple entities, proposes not just a single proposal for 100% of the funds, but multiple different proposals. The constituents of the voting bloc can achieve their goal of emptying out the fund piecemeal. Fundamentally, this attack is indistinguishable "on the wire" from a number of investment opportunities that seem appealing to a majority. The key distinguishing factor here is the conflict of interest: the direct beneficiaries of the proposals are also token holders of The DAO.

虽然 DAO 的白皮书曾经具体地提到过多数接管的攻击然后引进了监护者这个概念来制止这个攻击， 但我们不清楚这个制止机制是否真的足够有效。在白皮书里列出的多数接管攻击: 一个大的投票集团，有 53%以上的投票权，投票把 100%的资金拨给对自己集团有利的提议。监护者本来是应该发现这种行为来追踪受益者的身份。但是不清楚的是，如果这个集团是由多个实体组成的一个卡特尔，然后提出不是一个提议而是多个不同的提议，监护人是如何发觉这个攻击的? 这个投票集团里的成员可以用逐渐提离的办法来放空基金。最根本的是，这个攻击在一堆对大众看起来有吸引力的投资机会里几乎难以被决定性的分辨出来。最能够区别攻击的因素就是利益冲突：这些提议的直接受益者也是 DAO 的筹码持有者。

Reward Dilution

回报稀释

Another potential attack against token holders who split is for the remaining token holders of The DAO to dilute the dividends they pay out to token holders who split. They can carry out this attack by funding proposals that cycle the fund's coins, issuing new reward tokens that dilute the rewards that come in from earlier investments. This attack stems from the way reward accounting lumps maintenance costs, internal transfers and genuine investments into a single proposal abstraction. It requires curator participation to launch, but well-meaning curators can inadvertently launch it when reorganizing funds or when the fund fires underperforming contractors; that is, operations which take coins out and return them as rewards.

另外一个对分裂出来的筹码持有者的潜在攻击是剩下的 DAO 筹码持有者可以稀释他们给分裂出去人的分红。他们可以发起这个攻击来资助那些提议用来循环那些基金的币，发布新的回报筹码来稀释那些从以前投资里产生的回报。这个攻击源自回报会计计算把维护费用，内部转账和真正的投资都聚集起来放进一个单一的提议提象化。它要求监护者的参与来发起，但是有善意的监护者可能会不小心启动它当他在重组资金或是当基金把不符合服务标准的合同工解雇；也就是那些营运把币取出然后返回作为回报。

Risk-Free Voting

没有风险的投票

A token holder can vote on proposals without committing to fund them, which is an enabler for launching other attacks and executing strategic behavior. To do so, the token holder simply votes with his funds as usual, but then, when the voting period is over, calls 'unblockMe' and executes a split before the proposal is executed. This decouples the attacker's funds from any risk he might take with them while voting, and enables a large voter to force bad decisions on the remaining token holders as he exits. It is not without risk, as he may be unable to unblock and split in time, but it is nevertheless possible, as correct execution depends on timing assumptions.

一个筹码的持有者可以对于提议投票而无须承诺资助它们，这就让发起其他攻击和采取战略行为变得可能。为了做到这些，这个筹码持有者只要简单地用他的资金投票，但是当投票期结束之后，召唤“unblockme”然后在提议被执行之前执行一个分裂。这样一来这个攻击者的资金就会和他投票时的风险相脱钩，然后可以让一个大的投票者在他出局的时候把错误的决定强加在剩下的筹码持有者上。虽然他这样做不是没有风险，他可能不能及时分裂出去，但还是有这个可能，因为正确的行动取决于对时间上的假设。

The Concurrent Proposal Trap

同时进行提议的陷阱

The structure of The DAO can create undesirable dynamics in the presence of concurrent proposals. In particular, recall that a TDT holder who votes YES on a proposal is blocked from splitting or transferring until the end of the voting period on that proposal. This provides an attack amplification vector, where an attacker collects votes on a proposal with a long voting period, in effect trapping the voters' shares in The DAO. She can then issue an attacking proposal with a much shorter voting period. The attack, if successful, is guaranteed to impact the funds from the voters who were trapped. Trapped voters are forced to take active measures to defend their investments.

DAO 的架构可以在同时进行的提议的情况下产生不想要的状况。尤其是，回想一下在一个提议上投赞成票的 TDT 持有者要一直等到投票期过了之后，才能从那上面分裂或是转账。这就提供了一个加大攻击的矢量：这个攻击者可以在一个有很长投票期的提议里搜集选票，事实上把投票人的股份套牢在 DAO 里。她然后再发表一个有很短投票周期的攻击提议。这个攻击如果成功，就可以保证影响到那些被套牢者的资金。而被套牢的投票者则被迫采取主动措施来保护他们的投资。

Independence Assumption
独立性的假设

A critical implicit assumption in the discussion so far was that the proposals are independent. That is, their chances of success, and their returns, are not interlinked or dependent on each other. It is quite possible for simultaneous proposals to The DAO to be synergistic, or even antagonistic; for instance, a cluster of competing projects in the same space may affect each others' chances of success and thus, collective returns. Similarly, cooperating projects, if funded together, might create sufficient excitement

to yield excess returns; evidence from social science indicates that social processes are driven by non-linear systems.

到现在为止，一个重要但是隐藏的假设是这些提议都是独立的。这就是，它们成功的机率和它们的回报互不相连相互独立。同时向 DAO 提交的提议很有可能是互相促進的，或是相互反对的。举例说，一组在同个空间互相竞争的项目可能互相影响对方的成功几率，从而影响总体的回报；社会科学的研究显示社会上的成功是由非线性系统所推动的。

Yet the nature of voting on proposals in The DAO provide no way for investors to express complex, dependent preferences. For instance, an investor cannot indicate a conditional preference (e.g. “vote YES on this proposal if this other proposal is not funded or also funded”). In general, the construction of market mechanisms to elicit such preferences, and appropriate programmatic APIs for expressing them, requires a more detailed and nuanced contract. This does not constitute an attack vector, but it does indicate that we might see strategic voting behavior even in the absence of any ill will by participants.

然而 DAO 的投票机制的本质是没有给投资者提供表达复杂, 有依附性的优先设定选择。比如说，一个投资者不能够指定一个有条件的优先设定（投赞成票，如果其他提议没有得到资助或是得到资助）。总体上，市场运作机制的建立会引发出这种优先设定，然后相应的程序 APIs 来表达这些设定， 但这都需要一个更加细致和有层次的合同。但这都不构成一个攻击矢量，但它确实显示了我们可能会见到有谋略的投票行为即使参与者并没有什么恶意。

Potential Mitigations and Solutions

可能的缓减和解决办法

There exist partial and complete remedies to some of the attacks outlined above. Discussion of these solutions is ongoing. The mitigations and solutions require either technical changes to The DAO or a social agreement among The DAO’s curators, or both.

对上述的攻击有全部和部分的解决方法。在这方面的讨论正在进行。这些缓减和解决方法需要对 DAO 进行技术改造或是 DAO 监护者之间达成一个社会共识，或是两个兼有之。

Supporting Withdrawals
支持提款

A function that any token holder can call to have an instant and direct withdrawal of their share of the DAO’s Ether to regular addresses (and that would allow them to claim future rewards from proposals on which they already spent Ether) would make the Stalker attack impossible. It would also significantly mitigate the Token-Value attack.

一个筹码持有者可以召唤的功能是有一个迅速和直接提款，把他们在 DAO 里的以太份额直接转到一个正规的地址。（这样一来他们可以从已经花了以太币的提议上领取未来的奖励回报）。这个办法可以让跟踪者攻击变得不可能。它还可以显著地缓减筹码价值的攻击。

Many token holders currently seem to believe that they can withdraw from The DAO at any time. Guaranteeing that this can happen, without having to resort to complex defense mechanisms, will ensure that the token holders' expectations are met.

许多筹码持有者现在相信他们可以从 DAO 里随时提身出来。如果可以不动用任何复杂的防御机制就可以保证这点可以做到，那筹码持有者的期望就可以得到实现。

Post-voting Grace Periods

投票后的宽限期

Adding a grace period after the end of the voting periods, but before the proposals can be funded/executed, would give token holders time to move TDT or to split the DAO after seeing voting results but before their money is spent. Voting periods and grace periods would not be allowed to happen concurrently, because voting tokens must be locked until all of the voting periods for the proposals those tokens voted on.

在投票期结束之后加一个宽限期，但是在提议可以被资助或是执行之前，会给筹码持有者足够时间来移动 TDT 或是从 DAO 里分裂出来当他们看到了投票的结果。但是在他们的币被花掉之前。投票期和宽限期不能够同时进行，因为投票筹码必须被锁住一直到所有这些投票提议的投票期过了为止。

The addition of a grace period definitively solves the voting bias by allowing token holders to vote "no" without forfeiting their right to sell or split in response to the outcome. It also gives the curators time to defend the DAO against ambush attacks by un-whitelisting payment addresses after seeing the voting results. It significantly mitigates the majority takeover attack and the ambush attack, by letting token holders withdraw after the vote passes.

加上一个宽限期确实可以解决这个投票偏向：它可以让筹码持有者投反对票而不放弃他们根据结果来卖或是分裂的权限。它还可以给监护者时间来防护 DAO 不遭受埋伏攻击：当看到投票选举结果之后就把支付地址从白名单上拿下来。它可以大大地缓减多数接管攻击和埋伏攻击，因为它可以让筹码持有者在投票通过后提款。

Shorter Voting Periods

较短的投票期限

Shortening the voting period on a proposal so that the voting period only occurs in the last 1-2 days of a 14-day or longer debating period would shorten the time for which tokens are locked. This mitigates the Token-Value attack, and also reduces the propensity for voters to wait until the last minute to vote so that their TDT are not locked up.

缩短一个提议上的投票期限让投票期只发生在 14 天的最后两天，或是更加长的辩论阶段。这样会缩短被锁筹码的时间，来缓解筹码价值攻击，然后可以降低投票者为了筹码不被锁住而拖到最后一分钟才投票的倾向性。

Vote "No" and Withdraw on an Affirmative Decision

投反对票然后在一个肯定的决定上撤出

Having a special vote whose semantics are 'NO_AND_WITHDRAW_IF_VOTE_SUCEEEDS' allows token holders to signal that they will leave the DAO if a proposal passes. "NAW" votes publicly indicate that the voter believes this proposal would cause damage to the value of the TDT and no longer wants to be part of The DAO if it succeeds.

用一个特殊的投票，它的语法是"如果提议成功通过，就投反对票然后撤出'，这个特殊投票可以让筹码持有者发布信号，如果一个提议通过，他们就会离开 DAO。"NAW "选票公开表示投票者认为这个提议会对 TDT 的价值造成损害所以不愿意在 DAO 里待着如果它被通过的话。

Waiting for Quiet

等待不动的投票人

A potential defense to deter ambush attacks is to extend the voting deadline in response to last minute changes in the direction of the vote. While last minute votes are to be expected in a fair voting system, mechanism biases that incentivize token holders to sit on the sidelines can be countered by extending the voting period and giving people time to observe the direction of the vote and to participate.

一个阻吓埋伏攻击的可能防御是延长投票截止期来对付投票最后时间里的导向。虽然最后一分钟投票在一个公平的投票系统里是应该被允许的，但是运作机制的偏见会导致筹码持有者在一旁等待到最后一分钟。这个倾向性可以用延长投票期和给大家更多的时间来观察投票的方向来克服。

Commit/Reveal Voting

做出承诺/泄露投票

A generally applicable technique is to have the TDT holders first commit to their (blinded) votes, and then to remove the blinding in a revelation phase at the end of the voting period. This has the downside that the client voters now need to be stateful in order to remember their blinding factor. Further, they can share their blinding factors with others in order to reveal, and even prove, the disposition of their vote. Most importantly, blinding the votes diminishes the value of The DAO's voting process: by design, the votes can no longer act as a signal to other TDT holders about the holder's financial preferences. The preference discovery process will thus end up shifting out of the smart contract into exogeneous mechanisms, such as message boards and the like.

一个可以广泛应用的技巧是让 TDT 持有者先对他们（被遮蔽的）投票做出承诺， 然后在一个投票晚期的一个透露时间段里把这个遮蔽拿走。但这样做会有负面作用：一个投票人的客户端要有数据储存能力才可以记住他们的遮蔽元素。甚者，他们可以把他们的遮蔽元素与其他人分享来透露，甚至证明他们投票的倾向。最重要的是，把投票遮蔽起来会降低 DAO 投票过程的价值: 按照设计，这些投票不能够成为这些持有者金融偏好的导向信号。

这些偏好发现过程会导致脱离智能合约的领域而进入外来运作机制，比如象微博这种个人意见信息栏。

Vote Delegation

投票代表团

TDT holders who do not participate in the voting process reduce the security of the system. One can improve participation, and thus improve security, by enabling TDT holders to delegate their vote to proxies. This delegation feature necessitates significant modifications and sufficient complexity to render it unsuitable as a short-term fix.

TDT 持有人如果不参加投票过程会减弱系统的安全性。我们可以让 TDT 的持有者把他们的选票放权给他们的代理人这种方法来提高参与度，然后提高安全性。但这个代表的功能必须要大幅度改变系统还会十分复杂，所以它不是一个短期解决方案。

Reward Accounting

回报会计计算

The reward dilution attack can be stalled by a more accurate accounting of when each DAO split. Proposals can then pay dividends according to the number of reward tokens outstanding at the time they split.

回报稀释攻击可以通过一个对每个 DAO 分裂进行更加精确的财务会计计算被阻止。提案然后可以根据在它们分裂时候有多少还没有被清算的回报筹码来支付红利。

Curator-enforced Proposal Independence

监护者执行的提议独立性

The independence assumption may be maintained voluntarily by the curators by ensuring that the proposals that are eligible for voting at any given time are indeed independent from each other.

独立性的假设可以由监护者自愿维护。监护者要保证这些有资格在任何时候投票的提议是确实互相独立的。

Upgrading the DAO
DAO 的升级

The DAO (1.0) has a built-in upgrade mechanism called “newContract” that moves all the funds into a new DAO (1.1). While this mechanism is available, it might be prudent to save it for dire emergencies. A softer upgrade path might be to place a moratorium on new proposals, to create new DAOs, and then to provide proposals to shift funds from the 1.0 version to the 1.1 version (or versions).

DAO（1.0）有一个内置的升级机构叫做“新合同”。它可以把所有的资金移到一个新的 DAO（1.1）。虽然这个机制存在，但最好还是在万不得已的情况下再启动它。一个更加“软”的升级方法是暂时停止新的提议，制造新的 DAO，然后提出提案来把资金从 1.0 移到 1.1.

Summary and Suggestions
总结与建议

This paper outlined the operation of The DAO contract, which currently holds a substantial portion of the Ether supply and has generated much excitement about decentralized autonomous organizations and smart contracts. It also identified nine causes for concern, which might cause The DAO voters to deviate from a truthful strategy. Some of these behaviors have the potential to lead to financial manipulation and even loss. It finally identified some potential mitigations and solutions to some of these biases and vulnerabilities.

这篇论文讨论了 DAO 合同的运作。 这些合同现在拥有以太币供应里的很大比例然后制造了许多对 DAO 和智能合约的亢奋。我们还指出了九个令人担忧的理由，可能导致 DAO 的投票者会偏离真实投票的策略。有些行为还有可能导致金融操纵和损失。它最后还指出一些可能的缓减方法来降低一些偏见和脆弱性。

Given the concerns outlined above, we believe it would be wise for the curators to not whitelist any proposals until the DAO is upgraded to mitigate the potential attacks described in this paper.

基于上述的担忧，我们相信现在 DAO 的监护者最好不要把任何提案放入“白名单”。一个明智的选择是等到 DAO 升级到可以缓减可能发生的攻击的时候。

NOTE: THIS DOCUMENT DOES NOT CONSTITUTE FINANCIAL ADVICE. WE ARE NOT, AND WILL NOT BE HELD, RESPONSIBLE FOR YOUR FINANCIAL DECISIONS.

注意： 这篇论文不提供任何金融建议。我们不是，也不想为你做出的财经决定付任何的责任。

Acknowledgments

感谢

Many thanks to Rick Dudley, Christoph Jentzsch, Andrew Miller, Gustav Simonsson, and Alex Van de Sande for their comments and feedback on this draft. We are grateful to Toby Hoenisch, who pointed out the Risk-Free Voting technique, and Meher Roy, who discovered the token dilution attack and made it public.