源于区块链技术漏洞的数字资产盗用风险与管理改进

——以 The DAO 为例

曾雪云　陈泓旭　赵涔

摘　要：The DAO 是一个去中心化自治组织和区块链众筹项目，依靠智能合约和共识机制进行决策，因技术漏洞和管理缺失，导致 The DAO 的数字资产被盗、退出数字交易市场，严重挑战了区块链技术的信任基础。为确保区块链数字资产的安全性，本文以 The DAO 为例，从技术、运营和监管三方面对基于区块链技术的数字资产安全展开研究和提出管理建议。技术层面需要在程序编写和程序审查方面作出改进，管理层面需要建立技术风险监管机制，运营团队对可能存在的代码漏洞需要在风险排查和风险处理方面保持严谨性和高效率。

关键词：区块链众筹；技术漏洞；金融科技；The DAO
中图分类号：F820.3　**文献标志码：**A　**文章编号：**1003-286X（2022）16-0034-04

区块链众筹是指项目筹资方运用区块链技术公开发行加密数字资产（ICO）以筹集资金的融资行为，在技术范畴是一种基于公有链的分布式账本技术，各节点都拥有区块链上的完整记录，实现了去中心化和信任机制的重建。但倘若某个节点被恶意利用，数字资产信息就可能被篡改。2016 年因技术层面的代码漏洞而导致大量募集资金被意外窃取的 The DAO 事件，严重损坏了区块链项目的信任基础，成为区块链众筹项目的下行拐点。本文以 The DAO 项目为例，从技术、运营和监管三方面展开分析并提出改进建议，以期为区块链技术下的数字资产与财务管理提供借鉴和启示。

一、The DAO 项目的发展历程

（一）The DAO 项目的创设与特性

Slock.it 于 2015 年 11 月在德国成立，是一家致力于将以太坊区块链技术嵌入物联网设备和应用程序的金融科技公司。其宗旨在于通过区块链探寻物联网解决方案，因此也可以归为互联网科技企业。2015 年 6 月，Slock.it 认为去中心化分享经济极具前景，于是开始开发去中心化自治组织（Decentralized Autonomous Organization，DAO）的基本框架。2016 年 3 月，Slock.it 公司的创始人 Christoph Jentzsch 发布了 The DAO 项目白皮书，设想 The DAO 区块链项目可以摒弃线下实体管理模式进行线上智能化协作，并以智能合约的方式自动形成公司章程和构建链上自主治理方式。因此，The DAO 项目没有传统意义上的组织机构，而是一个完全去中心化的链上自治组织。就技术属性而言，The DAO 是一组在以太坊公有链上运行的智能合约；就财务属性而言，The DAO 属于众筹，投资人与发起人之间的财务关系在法律形式上是捐赠关系而非权益关系。此项捐赠的对价是 The DAO 公司发行的“DAO

基金项目：国家自然科学基金面上项目“金融工具准则变迁、公允价值会计与金融投资行为”（71872020）；
北京邮电大学 2019 年教育教学改革项目立项资助（2019JY-C03）
作者简介：曾雪云、陈泓旭、赵涔，北京邮电大学经济管理学院。

通证”数字资产，投资人将享有对应的受益权和投票权。The DAO 公司接受的捐赠资金将委托给为此项目设立的独立于发行人的基金会进行资金管理和运营。The DAO 项目于 2016 年 4 月进行了首轮的通证发行，顺利完成了首轮数字资产筹集。通过为期 28 天的众筹，The DAO 项目募集了约 1 150 万个以太币，当时价值约 1.5 亿美元。

The DAO 项目的首次发行成功主要有三个原因：一是具有去中心化特性。The DAO 项目的所有未来投资都将以集体形式表决，运营决策完全基于投资者的共识，这能够极大程度地减少和防范在中心化管理模式下易出现的经理层代理问题。二是资金利用率高于传统公司。The DAO 项目没有类似于传统企业的运营实体，因此减少了大部分实体组织所需的管理费用（如办公场地租赁、冗员负担、过度薪资、办公设备折旧等）。加之，项目的投资与结算以数字货币进行，免除了在证券交易所上市的交易成本，能够优化利用项目资金。三是具有高投资价值。DAO 通证不仅具有数字资产属性，还具有随时间推移持续上涨的权益增值属性，投资者可以在 DAO 通证上市后进行低买高卖的套利活动。因此，美国证券交易委员会（SEC）认定 The DAO 是一种通过以太坊筹集资金的风险投资基金，属于证券类资产，需要纳入金融监管。

投资者可用以太币（ETH）购买 DAO 通证，其既有货币属性，还有类似于股东权益的公司治理属性，可用于直接赞助和控制 The DAO 平台上任意形式的“提案”。基于预先嵌入区块链技术的智能合约，任何缴纳了最低押金的投资者都具有创建提案的权利，并按其具体出资额获得相应的 DAO 通证作为权益证明，以实现完全意义上的 The DAO 区块链社区自治。持有 DAO 通证的投资者可通过集体表决的方式决定提案通过与否，以实现对 The DAO 社区进行治理和运营，并从 DAO 通证的增值中获取收益。

（二）The DAO 事件的发生与终结

然而，The DAO 项目在发行后不久就因黑客的“代码套利”行为而宣告退市。2016 年 6 月，黑客利用 The DAO 智能合约漏洞，成功转移项目发行时募集的 360 万个以太币到“子 DAO”链中，企图将归属于社区投资者的通证占为己有。“子 DAO”链的设计初衷本是保护处于表决权弱势地位的代币持有者，给其一个小规模的可发起提议和组织投票的去中心化组织环境，但也因此给了黑客窃取区块链社区数字资产的机会。由于该“子 DAO”链有 28 天的锁定期（投票表决期），因此项目管理方有机会在投票等待期内通过发起一项新的表决而挽回损失，若能获得多数通过那么黑客将无法转移资金。

但事件的发展并没有像预想的那样解决，在等待期内为了阻止偷盗行为，以太坊的创始人 Vitalik 提出软分叉和硬分叉两个解决方案。软分叉是区块链或者去中心化网络向前兼容的分叉，新旧协议相互兼容，仍在一条链上工作；硬分叉则会使区块链发生永久分歧，在新的共识规则发布后，未升级的节点将拒绝验证升级节点产生的区块，此时就会产生两条链并且各自延续。在 The DAO 事件中，硬分叉也代表回滚交易，即把区块链中的数据恢复到过去某一状态。虽然硬分叉可以在“子 DAO”锁定期内将社区的相关交易回溯到被盗之前保全数字资产，但也会严重损害公众对以太坊区块链技术的信任。当软分叉提议公告发出后攻击暂时停止，但不久攻击者宣称给不支持软分叉的持币人以大额奖励，而后旨在侵占数字资产的网络攻击就再次开始。迫于形势危急，硬分叉方案在社区中获得大量支持并得以实施。

虽然最终挽回了资金损失，但硬分叉回滚交易的实施使得投资者对 The DAO 项目的去中心化数字管理的安全性产生质疑。社区成员开始意识到以太坊并非完全不受任何个人和组织的干预，而是处在以太坊开发者和运营者的控制之下，这意味着区块链众筹的项目开发者以及运营者群体事实上可以利用自身掌控的技术优势侵犯其他社区成员的利益。对于技术垄断和道德风险的担忧使得投资者对 The DAO 项目及其开发团队不再信任。2016 年年底，DAO 通证从各大数字货币交易所（如 Poloniex 和 Kraken 等）退出，宣告了 The DAO 项目的终止和失败。

二、The DAO 项目的资金风险分析

（一）技术标准的缺失

The DAO 项目失败的首要原因是黑客利用其智能合约中递归调用漏洞所进行的“代码套利”。递归调用漏洞是指攻击者通过频繁调用代码中的特定函数不断提取资金，实现在数字资产结算之前多次从 The DAO 资金池里重复分离出理应被清零的攻击者的数字资产。这说明当前电子货币市场的区块链技术还不成熟，代码编写的规范性还不足，并且缺乏统一标准。数字货币在本质上是一个电子记录，并不具有实物货币的独占性和排他性。记录若不能实时清零，就有可能产生

二次支付。但是电子系统中的结算和清算都有很复杂的代码程序，且有时延性，不像实物货币一样可以一手交清。攻击者正是利用了The DAO项目在代码编写上的不规范和技术漏洞，发起多轮次的数字货币提取并得逞。

针对区块链的网络攻击可以存在于基础网络层、平台层和应用层的任何环节，都可能引发技术风险并引起对技术信任的连锁反应。其中，应用层是区块链所有架构中最易发生安全性事件的一个层级。当前的攻击目标主要包括用户节点和数字钱包。在用户节点方面，黑客通常以在系统后台或者网页安装木马程序的方式侵入，从而谋求盗取或者胁迫转移数字资产。在数字钱包方面，恶意攻击者可以直接利用应用层技术漏洞来窃取用户的加密资产。

区块链数字资产项目存在技术安全风险有两方面的原因。一方面，当前区块链众筹项目缺乏统一的技术标准，开发者技术水平各异，暂时还没有能达成共识的代码标准，导致智能合约在编写的过程中存在缺陷；另一方面，项目开发者未进行充分的代码测试和审查就发布ICO项目，导致存在技术漏洞和被恶意利用的可能性。

（二）敏捷反应的缺失

警觉性不足与反应迟缓也是The DAO事件发生的原因。一方面，The DAO项目团队对于网络攻击未保持高度的敏感性和足够的谨慎性。保障加密资产安全性是ICO项目发行、后续运营和市场交易的重要因素，也是投资者信任运营团队和对代币资产保持信心的基础。相比以太坊雇佣第三方公司LeastAuthority、Dejavu、Coinspect进行安全审计，The DAO的运营者却并未采取任何审查措施。

另一方面，The DAO运营团队处理技术漏洞缺乏敏捷性。在新兴技术下，越来越需要敏捷反应。2016年6月漏洞被发现且被区块链圈广泛讨论的时候，项目团队就应加快系统优化和修补漏洞，而不是等到新版本上线再统一修改漏洞。但面对代码漏洞的争议与质疑，Slock.it的创始人Stephen Tual仍保持“没有资金风险”的态度，并未着力于系统检测和技术改进，而是出于安抚投资者情绪的目的表示会在即将发布的新版本中解决此漏洞。这种延迟行动错过了技术修补的最佳时期，致使在新旧版本更迭之前遭遇恶意攻击。开发者对于安全问题的大意和代码漏洞修复的迟缓，是The DAO事件发酵的最大成因。虽然区块链技术被用于解决代理和管理问题，但是技术背后的风险隐患很大程度上仍然来自于管理以及人的不足信和道德风险。

（三）技术监管的缺失

技术合规性监管机制的缺失也是The DAO事件发生的原因。与IPO项目受到严格监管不同，截至目前数字资产依然可以避免所在国证券交易监管和追查，使得区块链众筹项目成为法外之地。2018年1月，SEC和美国商品期货委员会（CFTC）联合发布《关于对虚拟货币采取措施的联合声明》，表明对虚拟货币尤其是证券类通证应实行穿透式监管，判断其项目性质并纳入证券范畴。但由于金融监管科技还在发展早期，行为规范、信息披露、法律法规都在探索之中，合规性管理、指引、标准依然缺乏，因此遏制恶意攻击和市场乱象存在困难。这导致大量区块链项目（如The DAO）并没有在健全的监管框架下运行，并且在受到恶意攻击后缺少应急处理方案或者危机应对机制。甚至在“The DAO事件”中，攻击者的代码套利行为在道德层面属于侵犯财产行为，但在法定技术规程上却很难判定为非法。

三、管理改进建议

（一）建立区块链技术代码标准和规范

除审慎周全的管理设计外，区块链众筹项目的稳定运行更需要技术的保障，但目前的区块链技术水平还无法完全保障数字资产的安全性。The DAO事件中由递归漏洞导致资金窃取的部分原因在于代码编写时缺乏统一的技术标准和完备的安全测试。因此，为保持区块链众筹数字资产的安全性，需要在程序编写和程序审查方面作出改进，以预防和减少技术因素带来的风险。

在代码编写方面，开发者团队应采用规范化的模型来设计编写智能合约，从技术安全角度规范区块链项目。在统一的规范标准下，一旦发生问题任意程序维护员都可以准确定位，避免由于团队间代码开发工具或标准的差异所引起的漏洞定位疏忽。外部市场也应建立统一的安全规范与技术标准，便于审计公司的安全审查和促进行业内安全检查程序在统一标准下的更新迭代。

在后续审查方面，区块链项目的相关软硬件应进行充分的安全测试以减少安全风险。内部需要建立技术风险监测机制，通过静态与动态相结合的校验器来检验运行代码正确性。同时运用数据加密和身份认证技术进行审核，增加区块链项目交易代码审查监测力度。外部需要委任审计公司进行多方安全审查和鉴证，通过交易安全审查和访问控制审查等查找

薄弱环节。

（二）建成敏捷反应的组织和控制系统

The DAO事件中管理团队的疏忽大意和反应迟缓，暴露出智能合约背后人为因素可能带来的安全隐患。区块链技术被用于解决代理和管理问题，但技术背后最突出的安全隐患还是管理上的不到位。运营团队在区块链社区讨论代码漏洞时未足够重视，对攻击者的恶意未足够警觉，也未及时进行程序优化，对网络投票参与人的私利心没有清醒的认识，这些都值得反思。因此，区块链项目需要在风险排查和风险处理方面保持警觉性和敏捷性，以减少网络攻击的风险和损失。

在风险排查方面，运营团队应高度关注潜在的安全隐患。第一，重视区块链社区的作用。运营团队需要在管理平台实时跟踪社区，搜索与查看是否有社区成员提出项目程序存在潜在漏洞的相关言论，并及时对所提及的漏洞进行检测与排查。第二，制定相应的内部控制制度。在团队内部设立专业的安全监管部门监控项目运行流程，建立内部控制规范，健全内部控制体系，不能因为有新兴的管理工具就取缔传统的管理机构，传统的以人为责任主体的内部控制规范体系依然是确保项目安全性和稳定性的基础。第三，采取应用程序白名单，对运行正确代码的交易程序进行授权。即对项目交易的合规性进行审计，确保只有被授权的程序才能运行，以防止恶意代码交易程序的执行。

在风险处理方面，运营团队可以运用新兴科技和事先制定的应急预案来敏捷应对。其一，发挥人工智能的自排查作用。运营团队对区块链项目的业务数据进行统计和分析，同时通过对可能的安全隐患进行分类，标注出每种类别的特点并训练机器进行风险自动识别。并且为机器设计自助优化程序，有助于部分常规漏洞一经识别便可被机器程序自动优化。其二，针对特殊风险事件制定应急预案。运营团队可针对当前其他区块链项目发生过和社区讨论提出的潜在问题，提前分类制定程序优化方案，并明确责任归属，根据问题分类制定保护级别。其三，制定特殊事项处理条款，赋予系统维护人员相关权限。在风险来临时准予他们自动获取处理权限，减少上级指示和批准的等待时间，以提高风险处理效率。

（三）建立适配新兴技术的金融监管机制

一是采用监管沙盒制度。监管沙盒是指金融科技公司需在经过监管部门对经营业务等的筛选后，才可进入项目预审批和投资试运行的一种监管模式。监管机构需要制定资格认定与发行标准作为监管沙盒试运行的初筛选条件，这可以在一定程度上减少金融创新的试错成本，并将更多的金融创新纳入过程性监管范围进行风险管控。

二是加强对新兴技术的监管。监管部门需要大力发展监管科技，借助大数据、人工智能、云计算等新兴技术替代传统的信息披露监管，重新构建金融监管体系，以实现对监管数据的触达、辨别和获取。通过引入自动化的金融监管科技，进行实时识别和数字资产跟踪，可以加强对区块链技术平台与区块链金融产品的合规性监管。

三是引入资金存管机制。在区块链项目中引入资金存管机制，将虚拟钱包存放在单独的类银行金融机构或者托管第三方机构的账户中，并定期进行账户检查，确保交易账户的真实性、与现有金融体系建立连接和有据可查。通过与主流金融体系建立连接关系，形成中心化监管体系，可以防范数字资产的偷盗和劫持风险，或在劫持后采取其他补救措施。

责任编辑　樊柯馨

主要参考文献

[1] 李爱君，张珺，赖翔菲，等. DAO调查报告——根据《1934年证券交易法》第21条第(a)款[C]. 金融创新法律评论，2017：175-189.

[2] 魏静娴，高舸帆. 区块链智能合约法律问题研究——以The DAO事件为例[J]. 法制与社会，2018，(15)：44-45.

[3] 丁文文，王帅，李娟娟，等. 去中心化自治组织：发展现状，分析框架与未来趋势[J]. 智能科学与技术学报，2019，(2)：202-213.

[4] 金璐，黄志华. 区块链技术下ICO行为的风险研判及刑法规制[J]. 北京理工大学学报(社会科学版)，2020，22(6)：123-129.

[5] 张毅，朱艺. 基于区块链技术的系统信任：一种信任决策分析框架[J]. 电子政务，2019，(8)：117-124.

[6]Mehar M. I., Shier C.L., Giambattista A., et al. Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack[J]. Journal of Cases on Information Technology, 2019, 21(1).