图片根源：由无界幅员 AI 工具生成

截至目前，在可编程区块链提供的所无效果中–平安、可预测性、互操作性和自主经济等–最普遍运用的区块链并不提供隐私，而这依然是其被普遍采用的一个关键阻碍。固然并非一切的加密代币都是地道的工具，并且可以在不时增加的 web3 生态系统中用于各种手腕，但区块链用户确真实区块链上运用数字资产相互买卖。大少数现有区块链的以后架构依托买卖透明度来促进怀疑，但这种默许的透明度和缺少隐私性增加了消耗者遭到损伤的风险，由于它允许其他区块链用户检查任何持有人的买卖历史和持有量。区块链的匿名特性是对不良行为者的维护，但它很冗杂被抑制。现代区块链剖析实践标明，对用户互动的启示式剖析可以用来穿透这种隐私，任何与钱包持有人中止买卖的人都可以有效地看到他们的整个财务状况。因此，固然它在追踪合法金融活动方面提供了辅佐，但买卖透明度使区块链技术的用户特地冗杂遭到狡诈、社会工程和不良行为者偷盗资产的影响，以及向第三方披露愚钝金融数据所形成的隐患。

区块链上公共账本的透明性与激进金融系统的默许隐私形成鲜明对比，后者发生于金融中介机构维护的公家账本上的买卖记载，并取得金融隐私权的法定权益和对愚钝金融音讯访问的人为掌握。梦想上，财政部负责美国金融制裁制度的外国资产掌握办公室（OFAC）和负责美国反洗钱法规和监视的金融立功执法网络（FinCEN）公布的法规和指南，以及它们的授权法规，旨在志愿透明度，以抑制激进金融体系的固有不透明性和它所提供的隐私。这些法规所发生的记载和演讲央求，央求金融中介机构坚持并向政府披露音讯（以及采取其他举措，如阻拦对资产的访问），以支持执法调查，阻拦惧怕主义融资，并促进国度平安以及其他事项。主要的是，这些措施为受维护的隐私权发明了例外，代表了隐私权和合规央求之间的平衡 —— 虽然是不完美的平衡。

关于公共区块链上的用户来说，这些保护措施都不具有 — 不论是公家账本固有的不透明性所提供的实际隐私保护，还是对金融隐私权的清楚法律认可。此外，试图引进的措施（如客户识别和尽职调查，俗称“KYC”央求）甚至有可以破坏匿名性所提供的最低水平的隐私，由于它发明了接收恶意攻击和外部威胁的“蜜罐”音讯。固然这些音讯的激进在保守的金融系统中会抵消耗者形成损伤，但它加剧了曾经具有的偷盗、狡诈、甚至人身损伤的高风险，而这些风险是由于完整的金融透明度而具有的。

固然有一些较新的、采用范围较窄的第一层区块链主要关心隐私效果，但关于那些实质上不具有隐私性的区块链，用户不得不依赖少量的协议和第二层区块链来完成交易数据的匿名化，而其中许多使用的是零知识证明及隐私保护的加密技术来完成

的。这些协议和区块链一般被指摘带有罪恶手腕（包括被贴上“混币器”的标签），不可招认的是，虽然它们的一局部数量与黑客和其他合法手段相关，但为合法手段促进保护隐私的技术是有不可招认的价值的。梦想上，这种技术可以让合法的消耗者受益于金融隐私和消耗者保护的水平，逾越保守金融效力的消费者所享用的程度。但是，最大限制地保护隐私的相同处置计划可以会阻碍政府为促进执法和国度平安手段而中止调查、打击合法金融活动或收回被盗资产的才干。那么，这能否意味着区块链技术肯定会唆使人们在检测、防止和破坏合法金融活动的合规性与隐私和消费者保护之间做出选择？

本文着重论证了答案能供认的。使用现代加密技术来处置这一抵触 —— 与现有的依托人为掌握的框架不同 — 不用定是零和游戏。谐和用户的隐私需求以及监管者和执法部门的消息和国度平安需求既是能够的也是必要的。本文提出了区块链协议中零知识证明的潜在用例，以实现这两组手段。首先，我们会描画零知识证明技术的基本原理，随后概述能够适用的相关法律和监控制度。然后，以 Cash 为例，我们列出了一些和政策制定者可以思索的初级处置计划。

在写这篇文章时，笔者肯定了一个次要的前提：“监管使用次第，而不是协议。”在美国，使用次第层使用天文围栏技术停止制裁选择，并经过各种措施限制用户访问，是一种稀有的做法。虽然这些限制是有辅佐的，但它们并不是万无一失的，不良行为者还是能够规避这些控制。因此，某些能够冗杂被受制裁方使用的隐私保护技术曾经在协议层面上归入限制，以处置国度安全效果。笔者不以为一切的隐私保护技术都应当做出十分的决议；开拓者应当有自在挑选能否要采用协议级的限制，以防止被合法分子使用和潜在的监管权益。关于那些选择采取保护措施的人，我们只是提供了潜在的替代计划供其思索，这能够会使这些处置计划愈加有效，同时也限制它们被用于检查的能够性。

假定不确保隐私，区块链技术就不可能实现主流采用。例如，当触及到金融基础装备时，假定用户的工资或其他愚钝的财务消息，包括医疗等效力的支付，都可以公开检查，那么基于区块链的支付系统的潜在用户可能十分不甘愿使用这些系统。此外，关于社交网络效劳、去中心化的借贷协议、慈善平台以及其他任何用户注重其消息隐私的用例，也是一样。

数据证明了这一立场。截至 2022 年 4 月 29 日，链上隐私保护效劳或协议收到的加密市场价值的 30 天移动平均值抵达了 5200 万美元，比之前的 12 个月增加了近 200%。为了了解状况，许多隐私保护协议使用算法加密技术，以促进区块链地址将数字资产取出相似的可替代资产池，随后由同一用户控制的另一个区块链地址从该池中提取相同数量和类型的资产，有效突破监管链，抑止交易的可追溯性。其中某些协议和一些二层区块链使用被称为零知识证明的算法来匿名化交易，而不把迟钝的用户消息流露在链上。

零知识证明使公共区块链上的公家交易成为可能。其中心是，零知识证明是一方（称为 "证明者"）压服另一方（称为 "考证者"）某项声明为真，同时不走漏任何使该声明为真的基础数据。例如，考证者可以证明对数独谜题答案的了解，而不走漏任何关于答案的信息。更诙谐的是，一团体可以证明他们的年龄契合买酒或投票的门槛，而不泄漏他们驾驶执照上的姓名和出华诞期。（从技术上讲，他们会在零知识中证明他们有政府签署的文件，而且他们在这些文件上的出华诞期肯定了这团体的年龄）。该证明使考证者置信这一梦想是真实的，而不泄漏任何其他信息。

人们可以使用零知识工具树立各种隐私机制。例如，爱丽丝可以把资金送到一个对交易细节失密的效劳机构，而该效劳机构会给爱丽丝一张放款收据。该服务和群众都知道爱丽丝发送了资金。稍后，当爱丽丝想从该服务中提取资金时，她树立了一个零知识证明，证明她有一张无效的收据，而且她还没有提取与该收据相关的资金。该证明没有透露任何关于爱丽丝身份的信息，但却让服务机构置信它正在与一个有资历提取这些资金的人停止交互。在这里，零知识证明被用来使服务置信提款要求是有效的，同时对提款人的身份失密。

主要的是，零知识证明经过允许选择性地披露评价政策合规性所需的信息，而不流露一切的基础信息来保护隐私。零知识证明可以实现不同程度的隐私，包括没有人可以跟踪交易的完整隐私，大约除了少数特定方之外对其他一切人的隐私。人们可能需求弱小的隐私保护虽然有许多合法的理由，但这些技术也可能成为接收坏人的要素。正如隐私保护协议的总体使用在 2022 年抵达高峰一样，从合法根源收到的价值的相对比例也是如此，往年到第二季度，非法区块链地址约占发送到此类协议的所有资金的 23%。虽然这些协议采用了保护隐私的技术，但区块链剖析公司，如和 TRM Labs，有时能够追踪流经这些协议的非法资金，由于它们没有足够的数额来掩盖这些活动，大约它们具有的数额不够多样化。此外，即使非法行为者使用隐私保护技术，他们依然面临着将其资产带出链外的应战，由于在大少数状况下，在全球主要金融中心和其他司法管辖区，出入金被金融机构监管，因此要遵守反洗钱/打击惧怕主义的要求。所以，虽然保护隐私的协议关于坚持合法用户信息的私密性至关主要，但它们确真实区块链生态系统中发生了破绽，供非法行为者应用。可以肯定的是，遵守国际法律和监控制度是冗杂的，但在去中心化的区块链协议中实施规范化和契合监管要求的零知识证明，可以处置一些关键的破绽，同时使 web3 参与者受益。

要理解零知识证明如何抑制合规性和隐私之间的清楚二元选择，需求理解与打击非法金融活动相关的特定司法监管要求。在美国，最有可能影响隐私保护协议的法规可分为两个次要的法律制度：(A)
依据一系列联邦法规和条例，一般称为《银行失密法》（BSA）–(i) 客户识别方案和客户尽职调查要求（一般称为“KYC”规范）和（ii)交易监测以及其他记载和演讲要求；(B) 总统战时和国度急切权益下的美国制裁方案。Web3 市场参与者必需

处理这两种制度的法律要求，以尽量增加因不遵守而被志愿实施的风险，并减轻对协议战争台的非法使用。此外，任何遵守规则的行为都可能招致严酷结果，包括民事奖励和刑事起诉。

BSA 要求某些金融机构和其他相关实体遵守一系列监测、记载和演讲权益。这些权益的目的是辅佐 FinCEN、OFAC 和执法机构辨认、防止和起诉洗钱、惧怕主义融资和狡诈活动，以及依据国度安全和外交政策目的辨认和封锁美国金融系统中属于被制裁方的资产。充沛遵守 BSA 和制裁制度，可以为监管机构和执法部门提供清楚和可审计的非法活动文件线索，对其胜利实施至关主要。

BSA 涵盖的或有权利的实体包括传统的金融机构，如银行，以及服务企业（MSBs），如货币交易商、兑换商和汇款商等等。此外，FinCEN 进一步廓清，发行、管理或兑换可兑换虚拟货币（CVC）或替代货币的价值的团体和实体也被视为 MSB，因而需求遵守 BSA 规则的所有适用合规权利。这是因为某些混币服务可以使替代货币的价值从平台内的钱包转移到平台外的钱包。相比之下，保护隐私的去中心化区块链可能不触及货币传输。正如 FinCEN 在其 2019 年公布的最新指南中清楚指出的那样，非托管的、自我施行的代码或软件，即使施行混币功用，目前也不会触发 BSA 权利。

相比之下，制裁合规要求的应用则不那么清楚。由外国资产管理处（OFAC）管理的制裁制度适用于所有美国人，包括团体和实体，不论他们寓居在哪里，并要求他们识别、阻拦和隔离触及受制裁方财富的交易。尽管OFAC表示，制裁制度自身并不适用于软件和隐私保护技术的发布，但假设不采取措施避免受制裁方滥用这些技术 — 如下文所议论的那样 –OFAC 的反应可能会破坏这些技术的可行性，例如最近Tornado Cash的状况。

那些业务方式被归类为 MSB 的团体或实体必需满意某些信息搜罗和交易监控要求，以施行 BSA 规则的权利。MSB 必需从使用其服务停止交易的人那里取得 KYC 信息，以核实这些人的身份。作为 KYC 次第的一局部，MSB 至少必需获得用户的姓名、地址和税务识别号码。

此外，MSB 还必需监测经过其平台停止的交易，并经过提交可疑活动演讲（SAR）演讲任何可能预示非法行为的可疑活动。BSA 要求 MSB 在知道或怀疑其平台上的交易可能触及非法活动时，必需在 30 天内提交 SAR，前提是该交易涉及的转账总额至少为 2000 美元。为了鼓舞及时申报，对某项交易准确申报 SAR 将使 MSB 免于承当与该交易相关的所有民事权利。

虽然 BSA 还对 MSB 提出了其他记载和演讲要求，如提交货币交易演讲（CTR），但这一要求目前并不适用于数字资产，因此与目前的目的没有直接联系。

FinCEN 完整有权管理 BSA，公布规则，并对遵守 BSA 的行为采取执法举措，但 OFAC 具有更普遍的司法授权。大少数经济制裁来自《国际急切经济权利法》（IEEPA）和《国度急迫外形法》（NEA）授予总统的权利。因此，制裁是经过行政命令制定的与战时和国家安全相关的权利。OFAC 监视美国的所有金融交易，并可制裁任何对国家安全形成威胁的个人、实体或国家。假设 OFAC 指定的个人或实体在经过任何美国人或实体（包括但不限于 MSB 和银行等 BSA 义务虚体）处理的任何交易或持有的财富中具有权益，则美国个人或实体将被要求 (i) 阻拦（解冻）被抑止的交易，以及与指定人员相关的任何账户或财富，和/或 (ii) 将收到的与此类交易有关的任何资金取出隔离的、被解冻的账户，并且（iii) 向 OFAC 提交某些演讲。在任何一种情况下，任何美国个人或实体都不得处理此类交易和/或释放此类资金，直到 OFAC 将相关个人或实体从制裁名单中移除、适用的制裁计划被撤销，或 OFAC 通过发放允许证清楚授权释放拘留的资金。

关于与加密交易相关的制裁，威望一般来自于专注于“严酷恶意网络活动”的 EO 13694。遵守经济制裁的个人可能面临民事或刑事奖励。应当指出的是，违犯制裁的行政或民事义务规范是严酷义务，这意味着即使故意这样做，也可能因发送或接收交易或未能冻结与受制裁个人、实体或国家相关的财富而承当义务。这实际上强加了一项失职调查要求，即在从事金融或商业活动时讯问资金根源。另一方面，刑事义务需求表现出故意为之，即违犯制裁的人故意这么做。司法部依据 IEEPA 或美国法典第 18 篇中编纂的洗钱法规对违犯制裁的行为提起刑事诉讼。但是，关于制裁义务和 OFAC 合规要求的主要结论是，这些义务适用于在美国或在美国展停业务的所有个人和实体，与个人或实体能否在 BSA 涵盖范围内有关。

零知识证明提供的增强隐私的潜力与上述监管框架具有抵触。该技术能够屏蔽交易细节，这意味着它可能不繁杂完整契合 BSA 要求等法规——尽管智能合约和代码能否以及在多大程度上受上述法规要求的约束仍是一个悬而未决的效果。如上所述，FinCEN 在其 2019 年指南中明白将软件代码从 BSA 的范围中豁免，因此，一个真正去中心化的协议不需求——甚至也不清楚它如何能够——搜罗和保管用户的 KYC 信息或文件 SARs。非常，管理施行任何制裁的授权法规和网络安全行政命令提到了目的个人和实体的“财富和财产中的利益”，这标明软件和计算机代码自身不在制裁的范围内。最近来自 OFAC 的指点方针似乎标明，发布软件自身并不是一种可制裁的活动。但是，依据 OFAC 对与 Tornado Cash 相关的某些智能合约地址的指定，这一结论还远不明白。

尽管如此，零知识证明可以想象为通过隐私增强协议减轻一些流露于非法金融活动和经济制裁义务的风险，包括减轻 OFAC 制裁试图处理的国家安全风险。特地是，以隐私为重点的协议可以实施多种措施来更好地管理这些风险，而不会削弱其有效性。下面总结了三种可行的措施，每一种措施都是在隐私保护协议 Tornado Cash 的背景下进行评价的。

证明零知识证明有潜力克制以后由隐私增强技术惹起的现有制裁制度下的潜在责任之间的二元选择的一种方法是通过Tornado Cash的镜头——最近被 OFAC 赞同的隐私增强协议。Tornado Cash 是布置在以太坊区块链上的一个协议，旨在匿名化用户资产，以保护他们的隐私。任何人都可以从他们的以太坊地址向 Tornado Cash 智能合约发送资金，这些资金将一直寄具有合约中，直到所有者选择提取它们。一般情况下，用户在放款前会等候几周、几个月甚至几年的时间，因为中间的时间段（在此时期其他用户取出和存款）可能会增加或增加 Tornado Cash 隐私保护功用的有效性。在放款时，该协议应用零知识证明技术将资金转移到一个新的以太坊地址，突破了资金最后取出 Tornado 的地址和事前从 Tornado 提取资金的新地址之间的联系。Tornado Cash 协议是不可变的、去怀疑的和完整自动化的。Tornado Cash 提供的匿名性依赖于多个用户同时使用该服务来断开用于存存款的钱包地址之间的衔接。此外，用户还保管了一份只需他们才干透露的证书，用以证明其寄存代币的所有权。与最近非法混币器使用率下降的趋向一致，Tornado Cash 平台也非常屡次地被用于洗钱。例如，在 2022 年 4 月对 Ronin 桥的黑客攻击中，大约 6 亿美元从桥上被盗，并转移到攻击者具有的以太坊地址。几天后，黑客将部分被盗资金转移到 Tornado cash。2022 年 8 月 8 日，OFAC指定 tornado.cash 网站和几个与该服务相关的以太坊地址，其中许多是智能合约地址，没有可识别的密钥持有人。财政部在发布这一制裁措施的公告中指出，有逾越 70 亿美元的非法支出通过 Tornado Cash 洗钱，其中包括朝鲜国家支持的黑客团体 Lazarus Group 洗钱的 4.55 亿美元，以及与 Bridge和Nomad Heists相关的少量资金。财政部选择对该协议及其智能合约采取举措，尽管对无辜的第三方形成了相当大的附带影响，包括阻拦未受制裁的个人提取使用该协议取出的完整合法资金。这个效果源于 Tornado Cash 的去中心化和非托管实质，这使得很难肯定对其活动负责的组织或个人。因此，在这种情况下，应用传统的制裁施行技术和阻拦财产利益可能带来技术上的法律应战。尽管此类协议有时被视为试图规避监管要求，但从网络安全的角度来看，Tornado Cash 的技术架构也可以代表弱小的隐私保护技术，以阻止未经授权的第三方和恶意行为者获取链上操作的个人和企业的迟钝信息。这种方法是首选的，并且在技术上可能远远优于传统的操作控制，这些操作控制限制对更集合的监管系统施加的信息访问，并且已证明越来越繁杂遭到恶意攻击和外部威胁。

财政部在与 OFAC

的声明同时发布的旧事稿中表示，“尽管群众做出了其他保证，但 Tornado Cash 一再未能实施旨在阻止其为恶意网络行为者洗钱的有效控制措施。”幻想上，正如下文更精细描画的那样，Tornado Cash 确实有一些技术控制措施，以避免该平台被用于非法金融活动。效果是——能否具有更有效的技术控制，例如应用零知识证明的技术控制，Tornado Cash 可以实施这些技术控制并压服财政部不采取它曾经采取的举措？让我们思索一下那些零知识证明处理方案，包括一些 Tornado Cash 实现的解决方案，以及其他可能提高效率的解决方案。虽然独自使用这些方法都不是灵丹妙药，但将它们区分起来可以提高检测、阻止和破坏非法金融活动以及受制裁国家行为者使用隐私协议的才干。它们是：(i）存款挑选——根据黑名单和容许清单反省钱包进行入站交易；(ii）提款筛查——根据黑名单和容许名单检查请求返还资金的钱包；以及（iii）选择性去匿名化——该功用可为联邦监管机构和执法部门提供交易信息访问权限。

以太坊区块链原生的数字资产或从另一条链桥接到它上的数字资产可以兑换成
并取出 Tornado Cash，以试图保护用户交易的隐私。为了避免资产来自受制裁的人员或与攻击或黑客相关的钱包，Tornado Cash 使用了依赖于指定地址“黑名单”的存款挑选。但是，“容许名单”的额外使用可用于解决国家安全效果，同时也可将协议合法用户面临的风险降至最低，如下文进一步概述。

黑名单

Tornado Cash 的存款挑选使其能够通过阻止来自美国政府制裁或以其他方式阻止的地址的任何拟议存款来自动限制谁可以使用该协议。Tornado Cash 通过使用区块链分析公司的链上服务来测试一个地址目前能否被指定在各种实体（包括美国、欧盟或区分国）的经济或贸易禁运名单（或“黑名单”）上。Tornado Cash 的智能合约会在接受资金进入其中一个池之前“调用”分析公司的合约。假设资金来自分析公司特地指定国民（SDN）名单上被屏蔽的地址之一，则存款请求将会失利。

虽然使用黑名单挑选存款是很好的第一步，但这种机制具有几个实际效果。首先，当网络立功分子从受益者那里盗取资金时，他们可以立刻将资金转移到 Tornado Cash 中，甚至在受益者见地到资金已经消逝之前，当然，也可以在分析公司将资金标志为被盗或出往常他们软件中的 SDN
列表之前。第二，如果网络罪犯的地址在取出 Tornado Cash 之前被列入 SDN 名单，那么偷盗者可以复杂地将资金转移到一个新地址，并在新地址被增加到制裁名单之前立刻重新地址将资金取出 Tornado Cash。干练的黑客团体，如朝鲜的 Lazarus Group，常有效地使用这些技术来避免被发觉。但是，区块链分析公司试图通过使用变卦地址分析和启示式方法来克制这一限制，以识别异样由指定团体控制的非指定钱包。最后，依托非政府实体作为关于制裁名单上的人或物的真相仲裁者，可能会形成难以查明和矫正的准确性效果。例如，一家分析公司可能会过失地

将一个地址列入黑名单，而目前还不清楚该地址的所有者是否有任何追索权来矫正这个过失（不像传统金融机构可以处理客户的表扬）。另外，由于所有的制裁都代表了政府的政策决议，因此还存在增加哪一份制裁清单的问题。

白名单

为了降低分析公司或政府实体可能应用黑名单不公正地检查违法用户的风险，隐私保护协议可能考虑一种更弱小的存款筛查方式，这种方式也依赖于存款筛查限制不适用的钱包地址的“容许列表”。该答应列表将包括与受监管的金融中介机构相关的钱包地址——如 这样的法币入口——这些机构将进行片面的 KYC 挑选作为其登陆进程的一局部，因此无需隐私保护协议来挑选这些地址，如下所示。

关于那些未包括在上述答应列表中的钱包地址，一种额外的存款挑选方法是检查提款时的预言机，并阻止受制裁地址或已被肯定为与非法活动相关的地址提出的任何提款。例如，假定一个非法行为者在黑客攻击后立即从一个地址向 Tornado Cash 发送资金。在存入时，该地址不在答应列表中，也没有被肯定与被盗资金或受制裁的个人或实体有关，胜利完成入金。但是，如果非法行为者试图在稍后的时间提取资金，并且在其间的时间段内，该地址被标志为与被盗资金有关或在制裁名单上，那么提取请求将失利。资金将坚持冻结外形，盗窃者将无法提取。这种方法有很多益处。首先，它可以防止窃贼使用 Tornado Cash 协议洗钱。其次，Tornado Cash 实施提款检查点起到了威慑作用，应当让不法分子清楚地知道，如果他们将被盗资金发送给 Tornado Cash，这些资金可能会被智能合约有限期冻结，从而阻止他们获得他们的成果。这样的威慑只会影响到网络罪犯，而不会影响 Tornado Cash 的违法用户。现实上，考虑到下面议论的存款时间段特征，以及非法行为者可能会将资金寄存在 Tornado Cash 中更长时间以最有效地匿名化他们的根源，这种存款筛选功用将非常有用，因为它能够筛选不时更新财政部制裁名单。

尽管提款筛查可以解决存款筛查的许多缺陷，但与存款筛查一样，它对任何必要的风险评价都黔驴技穷。此外，它会使 Tornado Cash 继续依赖区块链分析公司对制裁预言机的忠实操作。此外，与存款检查一样，还有政府检查的问题 – –
只需在提款检查的情况下，政府滥用制裁清单可能招致用户获得资金。

只要当存款地址（i）不在适用分析公司的 SDN 列表上（即，该地址不在屏蔽列表上）或（ii）从受监管的金融中介机构收到上述资金（即，该地址在答应列表上）时，该方法才允许用户在隐私保护协议中存入资金。该许可列表可以由控制协议的去中心化自治组织（ ）随时间进行管理和更新，也可以来自与受监管的金融中介机构相关的链上地址预言机（相似于 Chainalysis 运营的黑名单预言机）。某些隐私保护技术可以将这一概念进一步推进，将其协议直接衔接到受监管的金融中介机构，允许用户直接从这些中介机构将资金存入协议，而不需要先将资金转移到独自的

钱包地址。

同时使用黑名单和白名单作为存款筛选进程的一部分，与仅使用黑名单的方法相比有几个分明的优点。首先，被过失或恶意添加到黑名单的合法用户只需利用受监管的金融中介机构将资金存入协议，就可以避免检查。由于大少数非法行为者不应能够在受监管的金融中介机构开设账户，他们无法利用许可名单，将继续遭到审查，从而解决国家安全问题。此外，许可名单将改善所有受监管金融中介机构客户的隐私，因为它将保证他们能够享用隐私保护协议的益处，而不用担忧审查。

最终，尽管存款筛查有助于 Tornado Cash
施行阻止被遏止交易的义务，但对于可能被视为 MSB 并受 BSA 约束的其他隐私服务提供商，或许对于可能被要求对业务活动进行与制裁相关的风险评价的个人或实体，它不会提高这些实体为风险评价目的进行交易监测的才干。存款筛查是很好的第一步，但它不太可能完整增加对该协议的非法资金使用。

选择性去匿名化是满意潜在监管要求的第三种方法，它有两种方式：志愿和非志愿。

志愿选择性去匿名化

通过其存款收据功用，Tornado Cash实施了一种志愿选择性去匿名化的方式，它为以为自己被过失地添加到制裁名单的人提供了将其交易细节去匿名化给选定或指定方的选项。如果类似的自愿去匿名化功用与对不在许可名单中的钱包地址的提款筛查相分别，那么用户可以选择去匿名化他们的交易，而负责提款的 Tornado 合约将删除由于上述提款筛选进程而存在的任何妨碍。因此，用户将收到其资金，但用户不会从 Tornado 的隐私保护技术中获得益处，因为其提款地址分明会与存款地址链接在一同。自愿去匿名化将使 Tornado Cash 等协议能够解决提款筛选的某些缺陷（例如，无辜的用户不会面临资金被冻结的风险），但它也会降低提款筛选作为威慑的有效性，因为恶意行为者将能够仅通过吊销交易匿名化就从 Tornado 中提取资金。在这种情况下，非法用户将不会从使用隐私增强服务中得就职何益处。

非自愿选择性去匿名化

非自愿选择性去匿名化是一项额外措施，可以整合到 Tornado Cash
的智能合约中，使政府能够追踪和追踪非法收益。虽然 BSA
要求不太可能适用于非托管 web3 服务，但与区块链协议相关的可追溯性代表了一项关键控制措施，可以更普遍地防止包括受制裁方在内的非法金融活动。非自愿选择性去匿名化代表了一种弱小的工具，可用于保护授权目的的可追溯性，同时保护

隐私免受恶意行为者和未经授权的第三方的损伤。关键问题是，谁来保护解锁溯源的私钥？

一种解决方案可能涉及向中立的看门人组织或类似的受疑心实体提供私钥，并向政府当局提供另一个私钥。如果存存款交易不是来自许可列表上的钱包地址，则这两个私钥都需要去匿名化，而此类交易的细节只会透露给请求去匿名化的执法机构。看门人组织的作用是，在执法部门没有首先获得和提交有效的去匿名的授权或法院命令之前，抵御去匿名化。这不只使执法部门能够确定提供 Tornado Cash 提取资金的根源地址，从而允许政府施行其执法和国家安全义务，而且还将减轻政府持有密钥的担负，这对政府和 Tornado Cash 的用户都是次优选择。

这种方法存在一些应战。首先，不分明哪些实体可以访问私钥。目前还没有一个已知的运转中的看门人组织被树立来管理这样的进程。此外，还有许多管辖权问题。是否每个国家——甚至是专制政权——都有自己的私钥，让他们能够访问交易数据？如果是这样，如何确保这些政权不会将美国公民的交易匿名化？此外，看门人组织和政府当局将如何管理它们的密钥以确保它们不会被攫取？这些问题并不新颖。每次议论密钥代管时都会提到，而这就是非自愿选择性去匿名化。这种解决方案一直不受欢迎，而且充溢了操作上的挑战——也就是“后门”的概念。尽管如此，为了称心监管要求或增加将平台用于非法目的，这是开拓者可以考虑的一个选项。

针对上述挑战的一个可能的解决方案是允许用户在存款时期选择他们想要使用的公钥来加密地址。Tornado Cash 合约可能有多个执法公钥，比如每个国家一个公钥。在取款时期，用户可以根据所在辖区选择使用哪个公钥进行加密。用户可能需要提供其管辖权的证据，这将决议使用哪个公钥进行加密。该证据可以隐藏在零知识证明之下，因此除了相关政府机构外，没有人会知道提款的管辖权。实践上，这将解决专制政权获得交易密匙的问题，但它没有解决恶意政府以恶意（但不老实）的法律顺序为幌子，要求密匙持有者提供私钥的可能性。

对于那些有 BSA
义务的实体，选择性去匿名化将有益于保管提款筛选的监管可行性，包括能够进行 OFAC 规则的制裁筛选，以及能够搜罗 KYC 信息和交易数据，并可能提交 SARs 文件。此外，可以对上述非自愿选择性去匿名化方法进行改正，使两个密钥持有者只拥有 BSA 下特地要求搜集、保管和报告的信息的私钥（例如，KYC 信息和 sar），并且只能将这些密钥提交给 FinCEN 和 OFAC，或在提供有效法律顺序后提交给执法部门。这种方法将有助于确保用户数据的隐私，同时允许政府机构实行其监管职责。

为了让 Web3 技术在美国兴怒放展，隐私保护监管解决方案的展开至关重要。在制定这些方法时，零知识证明可以提供一个强大的工具，防止网络立功分子和友好国

家行为体将区块链技术用于非法目的，同时仍然保护用户个人信息、数据和金融活动的隐私。根据特定协议或平台的运营和经济模型以及监管合规义务，使用零知识证明可以通过存款筛选、取款筛选和选择性去匿名化，以称心这些义务，更好地保护生态系统不被非法使用，防止国家安全形成损伤。区块链范围活动的多样性可能要求开拓人员和考虑多种方法，包括本文提出的方法，以解决非法金融风险。

重申前面议论的准绳，即协议不应当被监管，开拓人员必须完全自在地选择是否要采用协议级别的限制来减轻这些重要的风险，笔者希冀这些想法在树立者和政策制定者之间引发创造性的议论、盘绕零知识证明的可能性进行进一步的研讨和开发。

原文链接