Orchid：去中心化的网络路由市场

Jake S. Cannell[1, 2]、Justin Sheek[1, 2]、Jay Freeman[2]、Greg Hazel[2]、Jennifer Rodriguez-Mueller[2]、Eric Hou、Brian J. Fox 和 Steven Waterhouse 博士。

版本 2.0
2019 年 11 月 18 日

1：第一作者。2：负责技术设计的合作者。
致谢部分中讨论了其他贡献。

摘要

我们推出了 Orchid：一种去中心化的匿名通信和虚拟专用网络市场。现有的隐私解决方案要么是伴随中心化风险的不透明商业服务，要么是免费的对等网络，缺乏正确协调的激励，无法大规模确保服务质量和经济安全性。在 Orchid 带宽市场中，节点提供商使用以太坊区块链质押代币，以此来播发他们的服务。通过选择经过随机权益加权并按照次要标准（价格、位置等）筛选的节点，客户端可以构建单跳或多跳洋葱路由环路。质押可以协调激励措施，防范运营商的不法行为；尤其是线性权益加权，可以压制女巫攻击。Orchid 采用概率支付系统，可扩展至每秒数百万笔交易，从而实现没有可信中央方的高流动性带宽市场。通过将交易方之间的隐性浮动余额降至极低的水平，数据包级支付可实现高频去信任交互。

1. 导言

互联网曾经是自由开放的前沿，如今却支离破碎，受到监视和审查。随着政府和公司越来越擅于监控、检查和阻止连接，对 VPN（虚拟专用网络）等隐私和匿名工具的需求已成为主流。尽管 VPN 在大多数使用情形下足够好用，但仍受制于基于中心化信任的模型的固有弱点。面对政府的强迫或额外收入诱惑，用户几乎无法保证他们的 VPN 提供商不会秘密地记录和共享数据。VPN 的重复付款和定价模型会造成锁定效应，使用户无法在一家提供商被封锁或速度缓慢时以极低的成本迅速改用其他提供商。当前的对等系统（如 Tor[1] 或 I2P[2]）通过构建多跳环路向任何一方隐藏路由信息。但是，这些系统是免费的，因此在性能和安全性两个方面都存在问题。由于激励措施不佳以及捐赠的免费带宽供应非常有限，因此性能和质量堪忧。攻击者只需很低的接管成本就可以提供很大一部分总网络带宽，所以安全性同样会遭受影响。

所需要的是采用适当经济激励和极微支付的对等隐私网络，使客户端能够通过来自许多不同提供商的统一全球节点池构建单跳或多跳路由。开放的市场体系可以确保由追求利润的卖方供应的带宽可以随着用户需求的增长而弹性扩展。加密货币合约机制的使用可以提供必要的激励，来防范恶意行为。

有几个核心挑战在推动我们的设计：流量分析、女巫攻击和随机选择问题。在详述 Orchid 本身之前，我们先简要介绍一下各项挑战。

流量分析

在理论和实践上，发送消息时很难做到不向接收方以外的各方泄漏任何信息。在 Chaum[3] 首先提出的*混合网络* 中，消息通过很多代理节点进行路由，这些节点在每一步都会随机重新排序，像信封包信封一样层层加密。*洋葱路由* 是 Tor[1] 采纳的一项后期发展成果，它对每个持久连接结合使用相同的分层加密概念和唯

一的随机代理节点路径（环路），而不是单个共享环路，以实现更大的可扩展性。*流量分析* 仍然是一个潜在的问题[4]，但可以通过带宽燃烧（填充）和/或随机消息延迟，付出显著的性能代价将其克服。*共谋* 是另一个严重的问题：如果环路中的所有节点中至少每隔一个都相互配合，它们就可以推断出整个环路。

女巫攻击

在任何开放网络中，代理都可以创建许多伪造的身份，表面上以大量独立节点的形式出现，实际上全都相互串通。要保持开放性，且与此同时防止单个攻击者在整个系统中取得压倒性优势，可能会很困难。解决此问题的办法之一是*工作量证明*，它源自 HashCash[4]，后来被比特币[5] 采纳，并在早期 Orchid 0.9.2[6] 中作为一种女巫防御机制被提出。工作量证明要求每个节点都消耗计算资源来证明其身份。因此，如果要创建大量伪造身份，将需要成比例地增加成本支出。*燃烧证明* 效果类似，但仅需要证明已销毁加密货币；它的优势在于，烧毁的货币的价值会重新分配给持币者，而不是完全浪费掉。基于*权益证明* 的加密货币要求用户质押货币以获取区块奖励并参与网络。我们使用一套*权益加权* 体系来挫败女巫攻击并协调激励措施，从而提供关键的经济安全优势。

随机选择

为了构建共谋可能性较低的安全环路，我们需要用一种对女巫攻击免疫的方式随机选择中继节点。我们通过线性权益加权随机选择来达成此目的，即*女巫正交*：攻击者无法通过将其权益分成多个身份来获得任何优势。这种选择方案还提供了一种简单有效的负载平衡方式，即使在最小的单跳环路（共谋不大可能发生）的情况下，也具有微妙的额外利益。实施全局随机选择策略要求客户端具有可用的节点元数据全局列表。为此，早期的 Orchid 0.9.2[6] 提出了基于自定义 Chord[7] 的 DHT（分布式哈希表）。为简单起见，我们现在直接使用以太坊区块链[8]（及其底层 DHT）来提供全局节点注册表。

概述

Orchid 是一种去中心化平台，利用该平台，客户端能够构成具有各种潜在用途的高性能洋葱路由环路，并在新的随机极微支付系统的支持下为此类环路提供资金。运行 Orchid 服务器软件的带宽提供商通过以太坊目录智能合约获取 Orchid 代币（“OXT”，一种兼容 ERC20[1] 的加密货币），然后将其质押以便获得与质押保证金规模成正比的流量和收入。客户端使用树数据结构，通过权益加权随机选择方法寻找节点；我们已将这种方法作为一种智能合约功能实现。然后，客户端使用概率极微支付为节点付款，发送频率为每秒一次。多跳环路可以每跳各使用一个账户，或通过间接洋葱支付转发来减少付款本身的信息泄漏。环路可能会因技术或经济原因而失败（例如，当客户端流量的环路特定成本超过其当前预算时），此时会进行重新采样。我们这一设计的核心机制非常简单，但是，关键在于细节。

2. 背景

隐私一直是网络领域关注的问题，尤其是随着我们的信息越来越多地在线转移以及每天都暴露出更多的漏洞，隐私问题显得更加严峻。

我们的很多基础性计算机网络协议[9] 和实践是在 1961 到 1989 年[2] 之间那种以学者和业余爱好者为主流的充满高度信任[3] 的文化中诞生的，至今仍在现代手机、笔记本电脑和台式机上使用。从根本上来说，所有这

[1] https://theethereum.wiki/w/index.php/ERC20_Token_Standard
[2] http://www.catb.org/~esr/faqs/things-every-hacker-once-knew/#_key_dates
[3] https://www.people-press.org/2015/11/23/1-trust-in-government-1958-2015/

些协议都未经过加固，并且对经济学视而不见。其默认运作机制就像是一个寄送大量机打明信片的邮件系统 — 缺少验证机制，而且有可能在中途发生无法检测到的修改或替换[4]。

互联网服务提供商 (ISP) 往往是公用事业公司，他们与威权政体[10] 合作[5]（或由其运营），同时操纵服务，以伤害用户为代价提高他们的收益[11]，并因此而背负恶名。虽然说 ISP 不大可能会自毁其数据传输服务的价值（也有一些例外[6]），但他们有可能破坏因为私有数据传输管道垄断的存在而导致形成的自愿性客户端/服务器双边关系，而学术界在最初设计这些协议时，肯定没有想到如何最大限度减少这一破坏。

即使在非威权国家/地区，有线电视公司、电话公司或专门公司也已开始游说代议政府将商业间谍活动[12]合法化，并公然违反与转发所有数据包相关的原始规范[13]。自 2014 年以来，Facebook 的热度急剧下降[14]（在 2019 年可见度最高的 100 个组织中排名第 94 位，略高于 Trump Org 和美国政府本身）[7]。不过，用户可以停止访问 Facebook，而他们已经开始这样做了[15]。相比之下，ISP 服务于低粘度市场，6,000 万美国人面临真正的宽带垄断[16]。

尽管已经尝试对主流协议进行加固，但很少有一般来说完全安全的发后即忘 (fire-and-forget) 协议（可以说数量为零）。例如，SSH 相对安全且得到广泛使用[17]，但在 2003 年发现了流量分析攻击[18]，而且截至 2019 年，用实代码对该问题的修补有很大的随意性[8]。

对于大多数用户而言，通过不可信的 ISP 路由器发送的未加固协议并不是一个紧迫的问题，但许多人确实会使用咖啡店、机场或酒店 WiFi 来访问互联网。在所有这些情况下，间谍活动、服务降级和价格欺诈比较常见，因为这些情况小规模重建了类似 ISP 的激励。当偶尔尝试免费的 WiFi 实现时，技术预算的减少可能会导致配置错误百出，结果意外导致用户互相监视。在公众看来，所有这些挑战和其他问题模糊在一起，让人模糊地感觉整个互联网，尤其是通过 WiFi 访问的互联网，以一种令人困惑和具有潜在危险的方式充满了间谍活动。

在企业界，虚拟专用网 (VPN) 技术最初被大规模采用是为了让员工（尤其是差旅中或远程办公的员工）从更广泛的（默认不可信）网络环境创建回到安全工作内部网的加密隧道。这种设置称为“VPN”，因为隧道软件使人们能够“虚拟”地位于其安全“专用网络”的“内部”。它并不能完全解决协议加固问题（流量的形状和时间往往不受保护），但通过这种隧道混合发送加固和未加固协议至少可以防止注入攻击，以及一些类型的推理攻击。

基本上，由于 VPN 服务在企业环境的兴起，相同的技术得以调整用途（使用类似的隧道概念），提供给了消费者市场。在这个新的生态系统中，没有雇主扮演本地可信机构的角色，从而导致技术人员、企业家和研究人员探索各种解决方案，从中寻找更可信赖的安全网络。在这一系列可能的解决方案中，消费者 VPN 占据一席之地，Tor 也占有一席之地，但是，改进 Tor 而做出的一些尝试多因激励和支付（或缺少它们）带来的挑战而告吹。

[4] https://en.wikipedia.org/wiki/Packet_injection
[5] https://en.wikipedia.org/wiki/BGP_hijacking#Public_incidents
[6] https://www.nicholasoverstreet.com/2010/03/new-wave-communications-the-worst-isp-in-america/
[7] https://theharrispoll.com/axios-harrispoll-100/
[8] https://zinglau.com/projects/ObfuscatedOpenSSHPatches.html

2.1 消费者 VPN

对用户来说，消费者 VPN 公司介入了 ISP 的工作。在此之前 ISP 有两份工作：(1) 安装线路和 (2) 不让这些线路上未加固的数据受到监视。而如今，ISP 只留下了第一份工作（他们能够保住这份工作是因为垄断着入户线路）。第二份工作一部分由 VPN 隧道软件（对数据进行加密）完成，一部分由 VPN 公司完成：将数据解密为加固程度较低的流，并将不同的子流转发到更广大的互联网的不同组成部分。

这些服务可以在很大程度上保护用户的流量免受不可信 WiFi 场景（如咖啡店、酒店、机场等）带来的危害。此外，在其他各种使用情形下，当客户希望向网站隐藏其 IP 地址和/或向 ISP 隐藏其流量时，这些服务也变得很受欢迎。

从许多隐私和信任模型的角度来看，当 VPN 大行其道状态时，实际上就变成了用户的新 ISP。但是，这意味着 VPN 提供商现在可以轻松地执行 ISP 以前能够实施的任何攻击。与其他中心化系统一样，VPN 的安全可信程度取决于控制他们的企业实体。此外，他们现有的支付系统和商业模式要求按月或更长的服务承诺，而短租会大幅加价，这造成了用户锁定。

2.2 Tor，洋葱路由器

寻求私有互联网连接的用户可以选择分布式系统形式的替代方案（大多数免费）。使用最为广泛的此类系统是 Tor 网络[1]。Tor 背后的核心理念是，在数据包到达最终目的地之前，通过多个随机选择而且在统计上不相关的中间路由器发送数据包，以此来混淆流量。

遗憾的是，像 Tor 这样的分布式系统自身也伴随着很多问题。主要问题之一是对良好网络行为的激励，如增加可用性和带宽，同时减少延迟。这些问题可以通过经济激励机制来克服。

分布式系统中的激励最初用于将简单的经济模型应用于系统，目的是推动良好的行为。早期的算法经常使用以物易物方式进行分布式资源分配，如投桃报李 (tit-for-tat[19])，利用诸如带宽和延迟等网络原语对奖惩进行建模。尽管这种方法通常可以带来稳定的分布式系统，但它们仍然经常遇到看似棘手的问题，如搭便车问题[20]。随着去中心化系统的发展，一种明确的对等激励经济奖惩方法开始兴起。这些方法为激励创造了明确的经济效用度量，从而允许采用微调方法来推动良好行为并抑制不良行为。

2.3 激励型 Tor

激励型对等隐私网络的最早示例之一出现在激励型 Tor[21] 中。Ngan 等人率先提出的这一方案建议将*投桃报李*策略作为一种激励机制来分配路由资源。投桃报李的核心是提供这样一种方式：对等方为你分配了资源，你也以同样的方式向其分配资源。如果对等方不合作，则你也不合作。如果对等方合作，则你也合作。通过这种方式，迭代决策的支付矩阵始终会产生纳什均衡。

最近，Androulakil 等人[22] 演示了实际支付如何可用来更加直接地鼓励数据包转发。概括来说，设计以匿名支付方案（用于支付路线中的第一个节点）和链式微支付（用于环路的剩余部分）的混合体为中心。这种设计意味着一个数据包转发市场。理想情况下，Tor 用户将倾向于选择为他们提供最佳私密性、带宽、吞吐量和延迟的对等方，为了换取他们的服务，将使用数字货币向他们付款。请注意，此时发送数据包的效用可以直接与金钱激励相匹配，而不必依赖于投桃报李模型中难以量化的支付矩阵。

尽管经济激励的核心理念对于推动对等系统中的理想行为有着难以置信的强大作用，但仍存在一些固有问题。也许，最大的问题是依赖中央银行铸造代币。如本文稍后所述，我们可以使用去中心化加密货币进行支付来解决此问题。

上述模型的替代方法之一是，通过 Ghosh 等人[23] 提出的带宽证明模型进行激励。在此模型中，环路中的每个对等方都帮助生成新的铸币证明，当向客户端发送足够的带宽后，客户端就会启动该过程。这些信息在链上进行广播，然后实际上为环路中的所有成员付款，作为转发数据包的报酬。尽管该协议在理论上似乎有效，但它依赖于通货膨胀来为节点付款，缺少市场驱动的定价，而且在抑制攻击和其他恶意行为方面有其他一些隐忧。

终极而言，在 Tor 中引入一种不会招致更多潜在攻击的高效激励机制似乎相当困难。

2.4 支付通道支持的路由

支付通道可同时用做发送信息和资金的路由。这方面的突出示例是由 Thomas 和 Schwartz 提出的跨账本协议 (ILP)[24]。ILP 中原子互换方法背后的核心理念是，使用哈希时间锁合约 (HTLC) 建立可加密验证的微支付通道，用于在转发数据包时支付代币。请注意，与传统支付通道不同，这些微支付通道相对较少在链上结算，从而同时实现交易费摊销和低延迟。但是，在此过程中，路由并不完全向网络隐藏。

Khosla[25] 在 ILP 基础上推出了一种基于洋葱路由的插件，可以实现与这些可加密验证微支付相关联的类 Tor 功能。他们的系统对多跳数据环路中的每个链路使用一个 ILP 支付环路，显著增加了延迟、错误概率和复杂性。

尽管支付通道支持的路由方法作为一种前景光明的去中心化支付第二层扩展解决方案引起了广泛关注，但由于需要执行递归路由，它们的部署和效率颇不理想。最终用户必须向一个或多个特定的支付路由器存入资金，因此需要信任并会引入一种交易对手风险。支付路由需要 O(log N) 步和延迟。付款并不总是可以路由的，具体取决于付款金额和关键边缘上的可用存款。如果关键边缘无法交付，支付路由可能会完全失败，从而导致长时间延迟。由于这些原因，支付通道网络通常并不是广泛采用的微支付解决方案，特别是对于洋葱路由来说。

3. 目标与局限性

Orchid 的使命是使人们能够了解和控制自己计算机的网络活动，而不必担心审查、监视或中介活动。为了实现这一使命，我们使用开源软件为广泛的受众构建解决方案，以求创建一个去中心化的 VPN 市场，并且利用基于以太坊区块链的概率极微支付为其提供支持。我们的设计强调可扩展性、去中心化、易用性、简单性和可延伸性。在支付匿名性、可扩展性和抗审查性方面，Orchid 继承了以太坊当前的一些局限性。此外，我们最初专注于可负担的高带宽、低延迟路由，导致目前限制了 Orchid 防御最复杂的理论流量分析攻击的能力。对于我们主要设想的大多数大众消费者使用情形而言，这些局限不构成障碍（第 6 节）。

3.1 目标

可扩展性

Orchid 极微支付系统可扩展到每秒数百万用户在当前以太坊区块链上每秒发送一次概率交易（第 5.9 节），通过使用以太坊 2.0 的分片功能，可能会扩展到每秒数十亿笔交易。节点选择过程（第 4.3 节）允许客户端以去信任的方式将节点选择工作外包给服务器节点，从而实现轻量级 Orchid 客户端实现。

去中心化

从极微支付到节点目录和发现，我们设计的所有组件全部去中心化。以太坊区块链用于执行功能市场所要求的最小一组合约结算。假设 OXT 权益均匀分配的情况下，Orchid 中不存在具有超大影响力或控制力的特别可信方。

易用性

易用性是广泛采用的关键所在，而系统为每个用户提供的匿名性也会随着用户群的规模而增加。我们的默认客户端实现可以“正常运行”，无需用户做出不必要的配置或路由管理决定（但有需要的用户可以获得详细的配置选项）。客户端还可以帮助自动执行一些繁琐的细节，如预算编制和节点选择。对于大多数用户而言，使用 Orchid 保护他们的网络连接几乎就像按一下按钮一样简单。

简单性

该协议易于理解、实现和进行安全性分析。我们使用销售商确定的带宽价格和客户价格过滤器，而不是更为复杂的拍卖机制。随机支付协议也比较简单：智能合约由大约 200 行 Solidity 代码组成。

可延伸性

我们的核心机制尽可能可以分离和正交，以便未来更轻松地扩展和替换。极微支付协议和智能合约不会直接与其他系统交互。同样，节点目录也是隔离的，并且与节点元数据注册表和其他组件分离。为保证容易适应，提款延迟等关键系统设计超参数被设成了合约参数。基于 WebRTC 的传输协议同样是正交且可扩展的。极微支付系统虽然是为 Orchid 带宽市场而构建，但却是通用的，具有广泛应用的潜力。

3.2 局限性

Orchid 建立在以太坊基础之上，后者从智能合约功能、去中心化、社区规模和参与度来看是世界领先的区块链。因此，我们有着以太坊固有的所有扩展和安全问题，但也可以依赖广大以太坊社区的努力来应对可能出现的任何危机。

网络依赖

Orchid 的经济安全性（第 4.4 节）上限取决于以太坊本身的经济安全性。有能力动摇或破坏以太坊网络的攻击者自然能够破坏 Orchid。（此外，对以太坊发动的任何成功的关闭攻击实际上也会关闭 Orchid，即使这种攻击是无意的）。例如，强大的攻击者可以通过发起持续的 51% 攻击来实现这一目标，而 DDOS 和其他针对关键以太坊节点的攻击还可能会放大这一攻击。

各个 Orchid 服务器节点也依赖以太坊网络，因为它们需要与以太坊节点的可靠连接来处理中奖的极微支付兑换。因此，各个 Orchid 节点也容易受到以太坊日蚀攻击的攻击。实际上，商用以太坊节点运营商（如 Alchemy 或 Infura）可以帮助减轻这些风险。

用户可扩展性

当前的 Orchid 极微支付系统存在效率/方差取舍：较大面值的彩币会牺牲方差来降低链上支付的频率，并减少交易费。我们预计用户对方差的容忍度有限。考虑到存在这些约束条件，并且以太坊当前的最大交易吞吐量约为每秒十几笔交易，这意味着扩展上限为数百万个 Orchid 用户（第 5.9 节）。利用以太坊 2.0 分片[9]，可以扩展到超越此用户数量限制。

支付匿名性

很少有中奖的极微支付彩币是通过链上以太坊交易进行兑换的。因此，Orchid 极微支付只是伪匿名的，有时会泄漏一些信息（第 5.8 节）。若用户需要更强的匿名性，则需要先将其 OXT 货币匿名化，然后再将其加载到极微支付账户中。

公共节点目录

Orchid 节点目录发布在以太坊区块链上，因此向世界公开。这样一来，从事审查的攻击者很容易自动封锁所有列出的 Orchid 节点联系 IP 地址。第 6.4 节讨论了具体的影响和可能的变通方案，如使用链下共享的私有 IP 地址。

流量分析

我们最初侧重于高带宽、低延迟环路，为此牺牲了强匿名性。这种取舍是基本的[26]，但我们的设计允许用户通过带宽燃烧方式，用带宽效率来换取更高的匿名性。

流量混淆

Orchid 的网络层基于 WebRTC 构建，后者提供了一定的初始混淆能力。但是，混淆和检测之间一直在进行研究上的竞赛[27]。高明的攻击者可以战胜大多数已知的混淆技术；我们寄希望于未来能够设计出更加强大的混淆插件（第 7 节）。

4. 市场设计

Orchid 市场是去中心化的对等 (P2P) 网络，它使运行 Orchid 客户端的用户可以向运行 Orchid 服务器的一个或多个卖方购买带宽，以便形成通往互联网上特定资源（如网站）的代理环路。

Orchid 市场中的主要参与者角色是：

- 运行 Orchid **客户端**的**用户**，他们将发起代理环路连接
- （可选）一个或多个**中继节点**，他们将转发加密流量
- **出口节点**，他们将最终连接外部目的地（例如，网站）
- **带宽销售商**，他们将接受极微支付以提供流量（中继或出口）

[9] https://github.com/ethereum/eth2.0-specs

带宽销售商在以太坊区块链上注册他们的节点，用户客户端则完全通过调用以太坊智能合约来选择适合的路由节点。Orchid 采用权益加权：销售商锁定 OXT 代币，构成与其节点关联的质押保证金，以便接收与其相对权益成比例的流量。

4.1 基本运作

概括来说，Orchid 市场主要开展以下运作：

- 为带宽销售商提供通过质押注册其节点的途径
- 为带宽销售商提供注册自定义服务和元数据的方法
- 为客户端提供向节点查询自定义供应服务和元数据的途径
- 提供一种选择随机节点的方法，概率与权益成比例，以便*女巫正交性* 属性得以保持（对于节点 X，质押规模 S 和乘数常量 α）：

$$P(select(X) \mid stake(X) = \alpha S) = \alpha P(select(X) \mid stake(X) = S)$$

女巫正交性需要线性选择属性，确保攻击者将其资源拆分为多个子账户后，不会在选择概率和最终的单位时间期望连接请求数方面占有优势；因此，女巫攻击将无利可图。如果给定这种线性加权选择属性，当有任意数量的攻击者在系统权益总和 S 中拥有总数为 A 的权益时，则随机选择的节点*不是* 攻击者的概率为：

$$P(select(\neg Attacker)) = 1 - \frac{A}{S}$$

权益加权的使用使 Orchid 网络的经济安全性可以随总存入权益的规模线性扩展，我们可以预计，此金额将在 OXT 总市值中占据相当大的一部分（下文第 4.5 节中详细分析了质押经济学）。权益加权选择过程本身是使用下文第 4.3 节中描述的链上树数据结构实现的，这样使客户端能够以可扩展的去信任方式将节点选择工作外包给其他节点，而不需要用轻量客户端下载、存储或处理完整的节点目录。

4.2 节点目录

Orchid 节点目录是存储在以太坊区块链上的一组数据结构，可以帮助客户端高效地选择带宽销售商的节点。本质上，它形成了以太坊网络上的一个简单的 Orchid 特定覆盖网络。节点目录合约提供了几个主要功能：

- **推**：此方法用于向特定的*被质押者* 质押*金额* 可变的 OXT 代币，然后增加到现有项中，或创建新的质押保证金项（与质押者、*被质押者* 相关联）。推功能还会使用*延迟* 参数，该参数将确定随后的提款锁定期。
- **拉**：此方法用于启动待处理提款，以便从现有存款项（与质押者、*被质押者* 相关联）中提取*金额* 可变的 OXT 代币。
- **取**：此方法用于在延迟期之后完成待处理提款，从而将被拉的资金转移到常规流动 OXT ERC20 余额中。
- **扫描**：此方法在给定随机种子参数的情况下，用于选择按照相对权益加权的随机节点。

节点元数据注册表

节点元数据注册表允许任何人使用元数据来“标记”节点。带宽销售商可以在区块链上使用它来存储与他们的节点相关联的自定义元数据，并播发服务，仅会受到以太坊交易费 gas 成本的限制。元数据注册表是通用的，可以为将来的自定义扩展提供一种简单的方法，从而使节点运营商能够播发新服务，然后客户端可以在不更新代码的情况下从中选择。

节点目录树

为了高效实现扫描功能，我们使用了链上二进制加权树数据结构。树中的每个节点都是一个权益项，用于存储被质押者、金额和延迟，以及左右子树的树指针和权益小计。这种结构实际上在所有质押保证金之上形成了一个前缀和树，可以在每个节点进行简单的下降决策，找到包含给定随机点的子树（或节点间）；只需要对数数量的步骤就能找到包含给定随机点的准确节点间隔。

提款延迟

提款延迟是一种重要的安全限制。它给试图获取大部分 Orchid 客户端连接请求的攻击者造成了障碍。我们尤其关心如何预防*系统性接管攻击*，在这种攻击中，攻击者会获取很大一部分的总质押保证金，然后将客户端定向到恶意服务器，而这些服务器会故意提供不良的连接、记录并报告流量或尝试发起主动连接攻击（例如，SSL 降级）。

与*权益证明* (PoS) 加密货币类似，我们防范系统性接管攻击的主要措施是建立高成本壁垒，阻止攻击者获取和锁定大部分 OXT 总权益。如果没有提款延迟，这一壁垒就会成为获取充足流动性的途径之一，攻击的实际净成本几乎为零。提款延迟为权益仓位制造了最小的利息或机会成本。成功的攻击还将破坏网络，并可能降低 OXT 代币的价值。因此，如果提款延迟足够长，那么攻击者最终结束攻击并出售大仓位 OXT 时，就更可能遭受额外的损失。

尽管底层机制大不相同，但短提款延迟 Orchid 中的系统攻击类似于工作量证明 (PoW) 区块链系统中的*租赁攻击*。Nicehash[10] 等哈希算力租赁服务的兴起带来了大量的哈希算力流动性，与购买必要硬件这一替代方案相比，它可以大大降低对 PoW 系统实施 51% 攻击的成本。攻击者已经通过租用哈希算力对许多小规模的数字币进行了双重支付攻击，甚至在 2019 年初成功攻击了排名前 20 的以太坊经典币 (Ethereum Classic)[11]。

理想情况下，提款延迟应长于我们预计市场发现并应对系统性接管攻击所需的时间。但是，较长的提款延迟也给希望减少或退出其质押保证金仓位的诚实带宽销售商造成了机会成本。关于这两个制约因素之间的理想取舍，很难进行先验估计，因此我们选择将提款延迟作为灵活的参数。然后，客户端软件将根据提款延迟进行*筛选*，忽略延迟低于客户端阈值的质押保证金。我们的初始客户端软件将接受 3 个月或更长的提款延迟，但是灵活的参数化机制允许未来通过客户端更新来更改此参数，而不会等同于硬分叉或产生相关的协调难题。

4.3 节点选择

客户端为代理环路选择节点时采用两步流程，先进行随机相对权益加权线性选择，然后进行次级约束条件筛选。第一阶段的线性选择由节点目录树上的扫描功能执行。客户端在本地生成一个随机点，并将其作为

[10] https://www.nicehash.com/
[11] https://cointelegraph.com/news/ethereum-classic-51-attack-the-reality-of-proof-of-work

要扫描的单个参数传入，然后沿节点目录树向下扫描。当单个唯一叶节点或节点间的权益段与选定的随机点相交时，搜索终止。

通过使用智能合约实现主节点扫描功能，可将选择过程轻松外包给节点。客户端可以请求一个或多个扫描调用，并让一个远程节点在本地执行每个扫描，然后使用以太坊 JSON RPC API[12] 的 eth_getProof 和 eth_getStorageAt 函数发回其正确性的简单证明。该机制将确保客户端能够可证明地信任节点未恶意选择自己或别名，并且就像客户端在本地对自己的以太坊区块链完整副本执行函数一样返回相同的结果。扫描功能的外包考虑到了轻量级 Orchid 客户端实现。

在根据线性相对权益加权选择一个或多个节点之后，客户端可以选择按照一些其他标准进行筛选，如退出地理位置、延迟/ping、节点白名单或自定义元数据标签。

地理位置

当前，VPN 的一种热门使用情形是绕过基于地理位置的内容过滤。诸如 Netflix 等流媒体服务采用国家/地区特定的内容许可证，并且通过检测用户的 IP 地址来实施这类许可。因此，位于正确位置的 VPN 或退出服务器可以允许访问原本被封锁的内容。

很难证明特定 IP 地址实际位于指定的位置。此外，出于合法的原因，客户端连接的最终服务器的 IP 地址可能与目录合约中列出的 IP 地址不同：大型带宽提供商可能将传入的客户端连接反弹/重定向到众多代理服务器中的一个，以实现负载平衡。由于这些考虑，对特定出口地理位置有兴趣的 Orchid 客户端可以使用已发布的节点元数据筛选所声明的地理位置，但最后必须检查最终退出连接是否确实位于所请求的位置。在某种程度上，可以使用地理位置数据库的公共 IP 地址自动执行该检查。

延迟

在某些使用情形下，我们预计用户希望连接的延迟低于随机选择的节点。与地理位置类似，客户端可以对延迟采用类似的猜测和检查策略。所声明的 IP 地址可对照公开的数据库进行检查，后者会将 IP 地址映射到位置以筛选掉远程服务器。最终，在建立路由后，必须测量实际的延迟。如果延迟高于目标阈值，则必须尝试新的不同路由。由于 Orchid 路由和极微支付的轻量性，可以快速设置和并行测试路由。

价格

由于卖方设定自己的带宽价格，客户端必须能够确定合理的价格水平，以避免费用过高。Orchid 客户端使用可定制的预算编制算法，根据用户的余额和其他参数（例如代表预算持续时长的目标时间跨度）确定当前的支出上限。例如，用户可以将价值 50 美元的 OXT 加载到他们的极微支付钱包中，并指示客户端将这笔钱作为一年内购买带宽的预算。然后，客户端软件使用此预算确定随时间支付的金额上限。如果客户端支付的带宽使用费低于服务器所收取的费用，则服务器将限制连接吞吐量。如果限制后的吞吐量低得不可接受，客户端将选择新提供商。因此，价格形成一个隐式筛选器，筛掉了带宽价格与客户端当前用量和预算消耗速度不相符的节点。

白名单

Orchid 客户端可以使用链上策划清单，该清单将可行节点筛选到自定义子集中。Orchid 客户端的官方初始版本将使用此功能，利用包含受信任 VPN 合作伙伴的默认出口节点白名单防止恶意出口节点发起的特定类

[12] https://github.com/ethereum/wiki/wiki/JSON-RPC#eth_getproof

型的攻击（例如 SSL 降级攻击）。定制的 Orchid 客户端可以使用自己的白名单，最终我们期望知名的第三方成为白名单策划人。白名单是引入外部声誉信任的一种简单方法，可补充通过质押实现的基于激励的经济信任。

自定义元数据标签

带宽销售商可以使用节点元数据注册表，来存储与区块链上各自的节点关联的任意元数据标签。将来，销售商可以使用它宣传新的自定义服务，例如专有 IP 地址。然后，用户可以设置客户端筛选器，按照关联的标签查找声称提供该服务的节点。虚假宣传（实际上不提供所声称的服务）的销售商有可能从热门白名单中除名。

4.4 权益加权的选择

Orchid 0.9.2[6] 的设计中以工作量证明 Medallion 作为反女巫攻击的主要机制，并明确反对权益证明。在本节中，我们将分析权益加权与其他替代方案，以及为什么我们改为采用类似权益证明的权益加权方法。

初步考量：攻击成本

像比特币、以太坊和大多数其他去中心化系统一样，Orchid 也是以开源软件为基础的开放式网络；任何人都可以下载 Orchid 节点软件，并在资源允许的情况下运行尽可能多的节点。在开放式去中心化系统中，防御系统攻击的可行措施最终必须具有*经济性*：系统的安全程度足以确保攻击者的攻击成本超过攻击所得的收益，或者高到根本无法执行攻击。

我们可以将经济安全分为绝对约束和相对约束。相对经济安全是指在任何资源加持下攻击都*无利可图* 的情况。绝对经济安全是指成本壁垒高，排除了资源不足的攻击者。比特币目前的绝对经济安全性是以数百亿美元衡量的。较小的新加密货币的绝对安全值可能低得多，但仍可依靠足够的相对安全性阻止大多数现实的攻击者。

工作量证明

工作量证明系统的安全性产生自在系统中证明有效身份而必须消耗的算力。Orchid 0.9.2 设计[6] 使用了基于求解每个新以太坊区块上播种的计算难题的 Medallion 机制，需要*连续* 的工作量证明才能维持当前的活动状态。因此，这些技术细节与比特币之类的工作量证明区块链系统非常相似。

如果我们假设工作量证明设计*不* 抵抗 ASIC，因此专用芯片的效率远高于普通芯片，*再* 假设上述芯片没有较大的租赁市场，那么工作量证明系统的经济安全约束大约为[28]：

$$N\,C > V_{sabotage} \qquad (3)$$

这里的 N 表示诚实（非攻击者）哈希算力总计，C 表示每单位哈希算力的总资本成本，$V_{破坏}$表示攻击者从系统破坏中获得的价值。方程 3 的 lhs 是攻击成本，也是绝对安全壁垒。

截至 2019 年中，比特币的 NC 价值以数百亿美元计。比特币的工作量证明规范不抵抗 ASIC，因此 ASIC 芯片凭借比可再利用的通用芯片高几个数量级的效率占据了主要地位。另一方面，以太坊特意设计了一种抵

抗 ASIC 的工作量证明规范。结果，ASIC 与已经称霸以太坊挖矿市场的通用图形处理器 (GPU) 相比优势极小。GPU 是通用的，所以存在流动租赁市场，而攻击者只需要在攻击期间支付哈希算力的租金即可。如果我们忽略攻击者在攻击过程中获得的区块奖励，那么需要 *t* 单位时间、每单位时间每单位哈希算力的租金为 *c* 的租赁攻击的经济安全约束大约为：

$$t \, \mathrm{N} \, c > \mathrm{V}_{\mathrm{sabotage}} \qquad (4)$$

攻击所需的时间 *t* 通常比硬件的折旧时间长度小几个数量级，所以租赁攻击情景导致经济安全性大幅降低。Orchid 0.9.2[6] 的工作量证明 Medallion 设计有意依赖抵抗 ASIC 的 equihash[] 方案。这在某种程度上是必要的，因为它要求 Medallion 必须由最终用户生成，而许多最终用户只有手机级别的硬件。ASIC 友好的工作量证明算法将赋予拥有 ASIC 的攻击者相对于拥有手机 CPU 的最终用户的巨大优势。遗憾的是，使用抵抗 ASIC 的算法意味着存在流动租赁市场，因此上述方程 4 的安全性较低。

花在工作量证明解题上的算力是一种浪费，就像在系统上相对于系统提供的带宽净值征收了一种税。每单位时间的收入 P 就等于带宽成本 B 加上维护 Medallion 所需的隐含计算成本：

$$\mathrm{P} = \mathrm{B} + \mathrm{N} \, c \qquad (5)$$

出于经济的考量将 N*c* 和 B 约束在相似的阶，否则比起替代方案，Orchid 对于消费者过于昂贵。将方程 5 代入方程 4 中，可得到安全性条件：

$$t \, (\mathrm{P} - \mathrm{B}) > \mathrm{V}_{\mathrm{sabotage}} \qquad (6)$$

举一个具体的例子：假设 Orchid 拥有 100 万用户，每个用户每年总共支付大约 63 美元（批发带宽成本加上隐含的工作量证明计算成本），并假设工作量证明开销大约是成本的 50%。因此，P - B 项只有每秒 1 美元左右。根据这些参数，攻击者只需花大约 3,600 美元租用算力就能捕获一小时内 Orchid 总流量的一半左右，或者只需花大约 86,400 美元租用算力就能捕获一天内 Orchid 总流量的一半左右。

权益加权

在我们目前的权益加权方法中，带宽销售商将 OXT 货币质押在定期存款中以证明身份，并收到与相对质押保证金规模成比例的流量。首先，我们将假设流动性足以支持攻击的 OXT 借贷市场不存在。为了控制 50% 的 Orchid 流量，攻击者必须获得并质押一定金额的 OXT，该金额等于非攻击者权益总额。成功的攻击将导致 OXT 的交换价值下降；攻击的主要成本是权益仓位损失。如果 S 是诚实（非攻击者）质押保证金总额，$\mathrm{x_d}$ 是攻击后 OXT 交换价值的最终百分比变化（预期为负），则相对安全条件为：

$$-x_{\mathrm{d}}\mathrm{S} > \mathrm{V}_{\mathrm{sabotage}} \qquad (7)$$

攻击成本和绝对安全壁垒就是 S（质押保证金数额），因为攻击者需要花费 S 数额的资本来执行攻击。

我们可以料想到，带宽销售商将学会根据市场情况增加或减少其质押保证金，以优化总利润。带宽销售商必须锁定 OXT 货币才能接收流量的这一要求意味着其资本的隐性机会成本。在竞争均衡环境下，我们可以预期流向带宽销售商的总收入 R 将大致等于带宽成本 B，再加上单位时间的机会成本（亦即利率 $\mathrm{I_r}$）与所需质押资本的乘积：

$$R = B + I_r S \qquad (8)$$

然后，总权益 S 可以用带宽成本、收入流和利率重写为：

$$S = (R - B) / I_r \qquad (9)$$

质押保证金资本的机会成本是一种形式的开销，其作用与工作量证明示例中消耗的算力成本类似。如果我们同样假设 50% 的开销，则机会成本等于带宽成本。使用前面例子中的参数，每年有 100 万用户购买价值 63 美元的带宽，50% 用于支付供应商的带宽成本，并假设每年的利率或机会成本为 10%，通过方程 9 可得出权益总金额 S 为 3.15 亿美元，这也是方程 7 中的绝对攻击成本约束。此值比使用连续工作量证明 Medallion 的攻击成本大三个数量级。

现在思考 OXT 权益租赁流动性市场存在的情况。我们可以首先想象一个金融市场，借款人提供另一种货币的抵押品，类似于空头头寸，但对资金用途没有约束。这种类型的租赁市场不会改变攻击成本和绝对安全约束 S，但是会导致相对安全约束的动态变化，因为攻击者现在可以避免 OXT 价值下降所带来的任何损失。

对于攻击者更有用的是无需抵押品即可直接租出质押保证金的市场。由于保证金是不流动的，因此承租人无法将其花掉，但可以得到质押保证金在 Orchid 节点流量上的全部好处。在这种情景下，攻击成本、相对和绝对安全约束改写为仅包含利息成本的流动方程：

$$t\, I_r S > V_{sabotage} \qquad (10)$$

在上面的方程 10 中，攻击成本现在只是攻击时长 *t* 内租用 50% 攻击前总权益（剩余“诚实”权益 S 的数额）的利息。将方程 9 的 rhs 代入方程 10 中的 S 同样可推出前面工作量证明部分中的方程 6：

$$S = (R - B) / I_r \qquad (9)$$
$$t\, (P - B) > V_{sabotage} \qquad (6)$$

因此，权益加权最坏的情况就是权益完全可租用，就像哈希算力完全可租用的工作量证明一样，都会导致安全状况恶化。

但是，撤回延迟参数对关键的攻击时间参数 *t* 设置了下限。使用前面的相同参数，100 万用户每年支付 63 美元，开销为 50%，则撤回延迟 3 个月会导致大约 790 万美元的攻击成本，这仍然比工作量证明 Medallion 的攻击成本高出几个数量级。

我们甚至可以建议增加质押撤回延迟，但是经济安全性不可能随着撤回延迟而单调上升。撤回延迟给退出权益仓位的诚实参与者制造了额外的机会成本，如果该成本太高，就可能会挤出原本很有竞争力的带宽销售商，这实质上就是通过提高有效利率 I_c 和/或提升带宽基本成本 B_c 而降低了总体效率。撤回延迟是最终由市场决定的一个可自定义的参数。

OXT 是一种专用资产，主要持有者没有动力将巨大的权益仓位出租给未经审查的未知实体。在这个意义上，OXT 的租赁动态更可能类似于比特币 ASIC 的租赁动态，后者可出租的哈希算力仅占总算力的一小部分。我们预期，白名单机制（第 4.3 节）可进一步打消权益持有者将权益租赁给不在同一白名单中的实体的想法（因为这样做可能会导致自己被除名），从而帮助保护任何权益租赁市场。这实质上将除名这一处罚（通过撤回延迟产生）强制从运营商承租人转移到了持有权益的食利者身上。

燃烧加权

我们还考虑了燃烧加权模型，其中将质押保证金替换为了可证明销毁的 OXT 货币。燃烧加权实际上等价于撤回延迟无限长的权益加权模型（质押保证金有效燃烧）。方程 7 中的仓位损失百分比项 x_d 成为 -1（因为全部仓位始终是损失的），所以方程简化为，攻击成本条件等于（已燃烧）质押保证金的总和。

因此，经济安全性不会随撤回延迟增加而单调上升的论断同样也适用于燃烧加权（撤回延迟无限长）。随着延迟的增加，权益持有者失去了资本保证金的选择权，因此会倾向于要求更高的有效利率以补偿失去的选择权。

由于燃烧加权已经是我们当前权益加权设计的参数模式，所以我们将来可以通过缓慢调高撤回延迟过渡到燃烧加权模式。如果客户端拒绝增加延迟，当然存在分叉或市场分割的风险，但是在理论上这种改变是非常可能实现的，而且我们将撤回延迟参数化的这一决策使其变得更容易。

利息加权

我们考虑的最后一种方案是替换直接权益加权，用撤回延迟期间的质押保证金有效利息或机会成本作为加权项。该设计背后的动机是通过更直接地补偿质押者与时间有关的锁定成本，来激励更多样化的撤回延迟。利息加权中的加权项将是这样的 $(1 - e^{(-w_t I_r)}) S$，其中 w_t 是可变的由运营商决定的撤回延迟，I_r 是全局“利率”参数，S 是质押保证金数额。

在这种利息加权设计中，关键设计参数 I_r 很可能设置为接近 OXT 质押保证金的实际市场利率或机会成本。如果利率项 I_r 远小于市场利率，就会激励参与者选择无限长（或最大限度）的撤回延迟 w_t，系统将退化为一种燃烧证明形式。如果 I_r 远大于市场利率，就会激励参与者选择非常短的撤回延迟，系统将类似于具有短撤回延迟的权益加权形式。

由于成功的系统性攻击将大幅降低 OXT 的价值，进而降低权益仓位，所以稳重的攻击者实际上承担极高的 OXT 利率或机会成本，因为他们认为 OXT 的价值将崩溃。所以假设利率项 I_r 接近市场利率，稳重的攻击者自然会选择非常长的撤回延迟，相对于权益加权，他们可以从利息加权中享受有效的攻击成本折扣。这是因为，在这种情况下大多数市场参与者将选择合理的撤回延迟以导致加权项显著小于 1，如此以来，相对于权益加权（攻击者将选择无限长延迟以使加权项达到 1），质押保证金总数额就降低了。

考虑到这些安全问题，还有朝着市场均衡方向调整全局利率参数 I_r 的一些异常复杂的未知动态机制，再加上在以太坊中实施复杂加权函数的一些问题，我们决定放弃利息加权。

总结

我们之所以选择权益加权设计，是因为它相对于我们早期的工作量证明 Medallion 设计有以下重要优势：

1. 工作量证明给最终用户造成了额外的计算负担
2. 即使假定在租赁市场中，工作量证明的攻击成本也远低于延迟权益加权的攻击成本
3. 一般的计算租赁市场的相对流动性已经远高于我们对未来任何 OXT 质押保证金租赁市场的预期
4. 权益加权可以留存带宽销售商的未来折扣利润，创造出更大的基线代币市值。下一节将探讨该主题。

4.5 代币经济学

权益加权相对于实用型代币系统的竞争机制能留存更高的价值，优势显而易见。在本节中，我们将简要介绍一些相关的经济假设并在分析后建立一个以用户极微支付保证金和节点质押保证金为主的简单模型。我们假设这些类别之外的任何其他价值要素（例如 ERC20 代币的短期高速流通）的贡献相对较小。

市场规模

我们首先了解这样一个场景，在系统总收入中，Orchid 有 200 万客户平均每月支付 5 美元或每年支付 120 美元。作为参考，到 2020 年全球 VPN 市场规模预计将达到 270 亿美元[13]。

用户保证金

我们预计大多数用户将使用足以支付至少三个月带宽费用的一些 OXT，来为其极微支付帐户预先存入资金，在本示例中为价值 15 美元的 OXT。VPN 用户已经习惯了预付数月或数年的服务费用，因为这已成为 VPN 市场中的标准支付模式。

因此，此示例中的用户保证金总价值为 3,000 万美元。

节点质押保证金

Orchid 是一个充满竞争的带宽市场，就此而言，我们预计系统最终将演变为总收入接近基本成本的近似均衡状态，其中，基本成本包括供应商的带宽原始成本以及质押保证金资本的利息成本或机会成本。回忆 *第 4.4 节* 中的方程 8 和 9：

$$R = B + I_r S \qquad (8)$$

$$S = (R - B) / I_r \qquad (9)$$

这里的 R 是总收入流，B 是卖方的带宽原始成本，I_r 是有效利率（机会成本），而 S 是总质押保证金。

现在许多权益证明加密货币系统的权益持有者通过运行节点赚取权益利息。每种代币的质押利率因系统细节、已知兑换风险等因素而存在很大差异。我们假设 OXT 权益的有效 APR（年利率）为 20%，这在质押收益率的典型范围内[14]。

IP 传输价格因地点而异，但合理的中位数估计为每月每 1 Mbps 1 美元[15]，也就是 1 美元/月传输超过 300 GB 的数据，大约每 GB 0.003 美元。我们将使用批发带宽价格 0.01 美元/GB。美国宽带家庭的平均每月数据使用量为每月 268 GB 数据[16]，因此我们将使用 100 GB/月作为每月每客户 VPN 数据的估算值。这意味着每用户带宽原始成本为 1 美元/月或 12 美元/年，由此得出一年的总带宽成本项 B 为 2,400 万美元。

因此，通过方程 9 可得知本例中的节点质押保证金总价值约为 48,000 万美元。

---

[13] https://www.statista.com/statistics/542817/worldwide-virtual-private-network-market/
[14] https://stakingrewards.com/
[15] https://blog.telegeography.com/yup.-price-erosion-is-still-a-thing
[16] https://www.telecompetitor.com/report-u-s-household-broadband-data-consumption-hit-268-7-gigabytes-in-2018/

诸如比特币之类的加密货币通常被用作*价值储存手段*。支持 Orchid 的 OXT 加密货币是在以太坊区块链之上实现的一种*实用代币*。虽然实用代币可用作价值储存手段，并且 Orchid 极微支付系统有可能在 Orchid 以外独立使用，但我们预期质押机制能够留存大部分价值。现在许多加密货币系统都有质押奖励，而 APR 收益差异很大。这些质押币的质押率（总质押保证金价值除以市值）也相差很大：Decred 的质押率为 50%[17]，而 NXT 的质押率为 15%[18]。

5. 极微支付

5.1 简介

如今，大多数第 1 层链上支付选项都面临易用性不足的问题，这主要与确认时间长、吞吐量低和交易费用高有关。例如，以太坊和比特币的确认时间分别为 15 秒和 10 分钟，交易费用约为 0.10 美元。[29] [30] 在 Orchid 网络中，我们将数据包传输（以及引申开来的带宽）与价值相关联。因此，如果传输数据包的交易费用和确认时间与当前第 1 层解决方案一样高，那么 Orchid 网络经济将彻底崩溃。简而言之，发送数据包产生的交易费用和确认时间不应比数据包本身的价值和传播时间高几个数量级。

我们的支付可扩展性要求自然建议使用第 2 层微支付解决方案作为网络的支付骨干。但是，由于数据传输与支付信息紧密相关，因此 Orchid 对带宽和数据包的保证也必须适用于支付。尤其是，Orchid 的目标是减少 Internet 监视和审查，这意味着数据传输协议和支付协议都应另外具有抗审查性、匿名性和去中心化或去信任性。下面，我们将这些用例需求分解为技术评估要点，以评估现有解决方案和我们提出的协议能在多大程度上解决 Orchid 核心支付挑战。

可扩展性：系统必须支持数百万个频繁进行微小交易的用户（大约每秒一次），这意味着每次支付的预期交易费用可忽略不计。

去信任性：系统不应要求参与者信任特定的实体，以免功能依赖于特定的性能和信誉。

匿名性：支付应极少泄漏现实身份的附加信息。此外，系统中的所有各方都需要能够拒绝可疑的资金发送、接收或传播 [31]。

不可审查性：攻击者审查交易的费用应极其高，这意味着损坏信息或阻止信息访问或发布从经济上或密码学上看总体是不可行的 [31]。也就是说，除非大部分网络由试图审查支付或数据包的恶意行为者控制，否则应该可以找到某种方法在不损坏任意端点的情况下汇款和收款。

在以下各节中，我们将讨论现有的支付解决方案、它们与以上评估框架的符合程度，并证明 Orchid 的支付框架可以比现有解决方案更好地为特定用例提供保障。

5.2 现有解决方案及其对比情况

如上所述，转移与任意带宽数量关联的价值（可能低至数据包级别）的前提条件是拥有一个强大的微支付基础架构，其中第 2 层解决方案最为流行。第 2 层解决方案将链上支付的安全性与不直接牵涉主区块链的协议绑定在每个交易中。从理论上讲，由此可带来很多好处，包括降低交易费、确认速度更快等。遗憾的

[17] https://stakingrewards.com/asset/dcr
[18] https://stakingrewards.com/asset/nxt

是，当今的生态系统中尚没有可用于生产环境的微支付解决方案。我们将根据*第 5.1 节*介绍的关键评估要点探讨现有方案的失败之处，继而提出一种全新的随机价值交换极微支付协议。

5.2.1 集中支付

传统的金融支付交易是通过各方之间的谈判来达成的，例如银行或支付服务提供商之间的谈判。这些交易通常是通过集中协议执行的，例如适用于支付卡的 ISO/IEC 7816 [32]、适用于工资单和信用转帐[19]的 ACH 或适用于 ATM 交易的 NYCE [36] 和 SWIFT [34]。这些网络中的参与者混合使用电子支付收据和手工调账 [37]，以使本地分类账与中央网络同步。

遗憾的是，集中支付系统不能支持*第 5.1 节*中枚举的大多数要求。集中式金融生态系统中盛行的欺诈 [38] 以及反欺诈解决方案（也就是逆向交易 [39]）都分别违反了*去信任*运营原则。尽管集中式系统中的响应能力极高，但拜占庭容错能力不足而且子系统之间缺乏互操作性，意味着全局系统中只有一部分可用，同时还存在一致性问题。最后，参与和管理支付基础架构的受信方通常掌握有关每笔交易的详细元数据（发送方、接收方、金额和时间），因此具备从事和遵守审查与去匿名化的所有必备要素 [40]。

Orchid 0.9.2 [6] 中提到，集中支付的交易费差异很大，少至支付卡交易的几分钱 [41]，多至国际电汇的 75 美元 [42]。作为替代或补充，许多系统会收取一定百分比的费用，从支付卡的 3.5% [43] 到银行转账的 13% [44] 不等。固定费用一般不适用于微支付，但按百分比收费的系统可以为微支付提供合理的支持。特别是，亚洲采用的微信支付和支付宝证明了按极低百分比收费的商业可行性，通常在 0.0%-0.1% 之间 [45]。遗憾的是，这些系统仍然存在先前提到的所有集中化缺陷。

F 表示功能齐全，P 表示有部分功能，N 表示无功能

可扩展性	去信任性	不可审查性	匿名性
[N, P, F]	N	N	N

5.2.2 支付渠道

支付渠道是一种较新的第 2 层解决方案，可纵向扩展传统第 1 层区块链系统的安全性和保障性。比特币上的闪电网络 [46] 是探索此类解决方案的首批协议之一。在抽象级别上，大多数支付渠道包含三个步骤：将资金锁定在第三方存管机构中，使用这些资金进行链下交易，在支付渠道关闭后将最终状态广播给第三方存管并向两个渠道参与者付款。

但是，现有的支付渠道基础架构存在许多问题，因此无法在 Orchid 网络中顺利使用。首先，支付渠道的资金路由很复杂，发送和接收资金平均需要 $O(log(n))$ 跳，其中 n 表示网络中的节点数。虽然端到端支付路径中的每一跳对于网络的成本都非常低，并且主要集中在路由/计算成本上，但整个路径也会成对地产生支付渠道的建立和拆除成本。与此紧密相连的问题是，如果网络中的一跳支付失败，可能触发超时，致使整个路径停顿。这意味着 $O(c * n)$ 建立和拆除的复杂性平摊在支付渠道的平均生命周期内，其中 c 表示每个节点维护的支付渠道数量。此外，还有资金的冻结成本；当资金被锁定在支付渠道中时，将无法在其他地方使用。当一个人希望与多个节点建立对等关系时，这就会产生问题；一个节点不能使用所有代币向任何对等方进行微支付，而是每个锁定的代币只能与一个对等方进行交互。

[19] https://en.wikipedia.org/wiki/Automated_clearing_house

请注意，支付渠道通常是使用哈希时间锁定合同 (HTLC) 相对于根链加密执行的。支付渠道的交易费用通常也很低。支付渠道的可审查性有点微妙。在比特币网络中，Heilman 日食攻击分析 [47] 表明，仅使用 400 个 IP 地址对比特币节点发动日蚀攻击是可行的（概率 $> 50\%$）。为了对支付渠道实施此类攻击，必须让一个节点无法与更大的 L1 网络进行通信。这在很大程度上取决于对等关系的实际处理方式，因此日蚀攻击的复杂性因 L1 平台而异。至于匿名性和隐私性，很遗憾，这两个属性在当前的支付渠道技术中非常有限。

F 表示功能齐全，P 表示有部分功能，N 表示无功能

可扩展性	去信任性	不可审查性	匿名性
F	P	P	N

5.2.3 概率微支付

概率微支付的概念是 Wheeler [48] 和 Rivest [49] 在上世纪 90 年代末为了减少交易费用对传统微付款的影响而提出的。Pass 和 Shelat [50] 在 MICROPAY1 中将这一想法扩展到基于区块链的支付系统，以使去中心化系统同样受益于此。此类微支付的核心思想与支付渠道类似：将交易费成本平摊到众多的交易中。但是，区块链支持的概率微支付的核心机制不是 HTLC，而是采用了基于彩币的支付。在这样的系统中，$\$X$ 付款实际是作为“彩币”发送的，票面价值为 $C * \$X$，中奖概率为 $\frac{1}{C}$，因此彩币的预期价值为 $C * \$X * \frac{1}{C} = \$X$。

该方案可大致描述如下：

A 想要付款给 B
A 将一些货币存入新生成密钥的比特币第三方存管地址 h_E
B 生成一个随机数 R_B 并将隐藏签名的承诺传输给 A
B 还将收件人地址 h_B 发送给 A
A 生成一个随机数 R_A 并以明文签名，连通支付信息一同传输给 B
如果 $R_A \oplus R_B$ 以 00 结尾，并且 R_B 符合隐藏签名的承诺，则彩币中奖，第三方存管机构兑付给 B

根据设计，该方案理论上是可扩展的，而且交易费用可以忽略（因为几乎完全是链下交易）。遗憾的是，在实际操作中，大多数现有方案都依赖于协议中某个位置的中央中介，因此它们并非是去信任化的。此外，在审查阻力方面，上面的支付渠道小节中提到的日蚀攻击问题也同样出现在这里。概率微支付和支付渠道之间的最大区别是概率微支付的 O(1) 支付路由复杂度。

F 表示功能齐全，P 表示有部分功能，N 表示无功能

可扩展性	去信任性	不可审查性	匿名性
F	P*	P*	N

** 受到现有实施方案的限制*

5.3 Orchid 极微支付方案

Orchid 极微支付方案从*第 5.2.3 节*简要提到的 Pass 和 Shelat [50] 的 MICROPAY1 方案概念中获得重要启发。我们支付系统的理念试图基于 MICROPAY1 方案进行合理的迭代，一个特别目的是让系统以可忽略不计的

安全成本实现经济的可扩展性。为此，我们创建了一个协议，旨在满足支付系统的可扩展性、去信任性、不可审查性和匿名性要求。

我们基于这些属性描述了 Orchid 极微支付方案。为此，我们提供了以下定义：

行动者：

发送方：极微支付的发送方。发送方应该拥有一个以太坊账户，并能够连接到一些以太坊节点以建立极微支付账户并向该账户注资。发送方在收到包含接收方的哈希承诺和目标账户的消息后，通过向接收方发送彩币（见下面的定义）来提交付款。

接收方：极微支付的接收方。接收方需要一个以太坊账户并能够访问一个以太坊节点。接收方生成一个哈希承诺，将其与目标账户 ID 一起发送给发送方，然后接收发送方的一个或多个彩币。接收方负责确保发送方收到正确的支付参数并拥有所需的资金。

支付/会员智能合约：该智能合约负责解决任何中奖彩币的支付过程，还强制执行加密经济激励措施，以防止发送方实施抢先交易、恶意破坏、双重支付和其他恶劣行为。

消息：

随机承诺：彩币接收方最初为提交随机生成数而发送给发送方的承诺消息。该承诺通过哈希函数隐藏了随机数。

彩币：为完成交互式彩币生成过程，发送方发回给接收方的消息。这包括发送方的随机数和签名，用于确认完成的极微支付的关键字段。请注意，彩币的有效值是其预期值。如果彩币中奖，则真正的赎回价值就是发送方和接收方商定的面值，否则就是 0。当且仅当彩币生成过程产生的随机数满足结算条件时，彩币才会中奖。

中奖彩币：完成的极微支付，满足按给定面值结算的条件，特别是包含满足中奖概率的随机数。这条消息广播到以太坊网络，要求发送方的支付第三方存管机构进行结算，或用于证明恶意破坏。

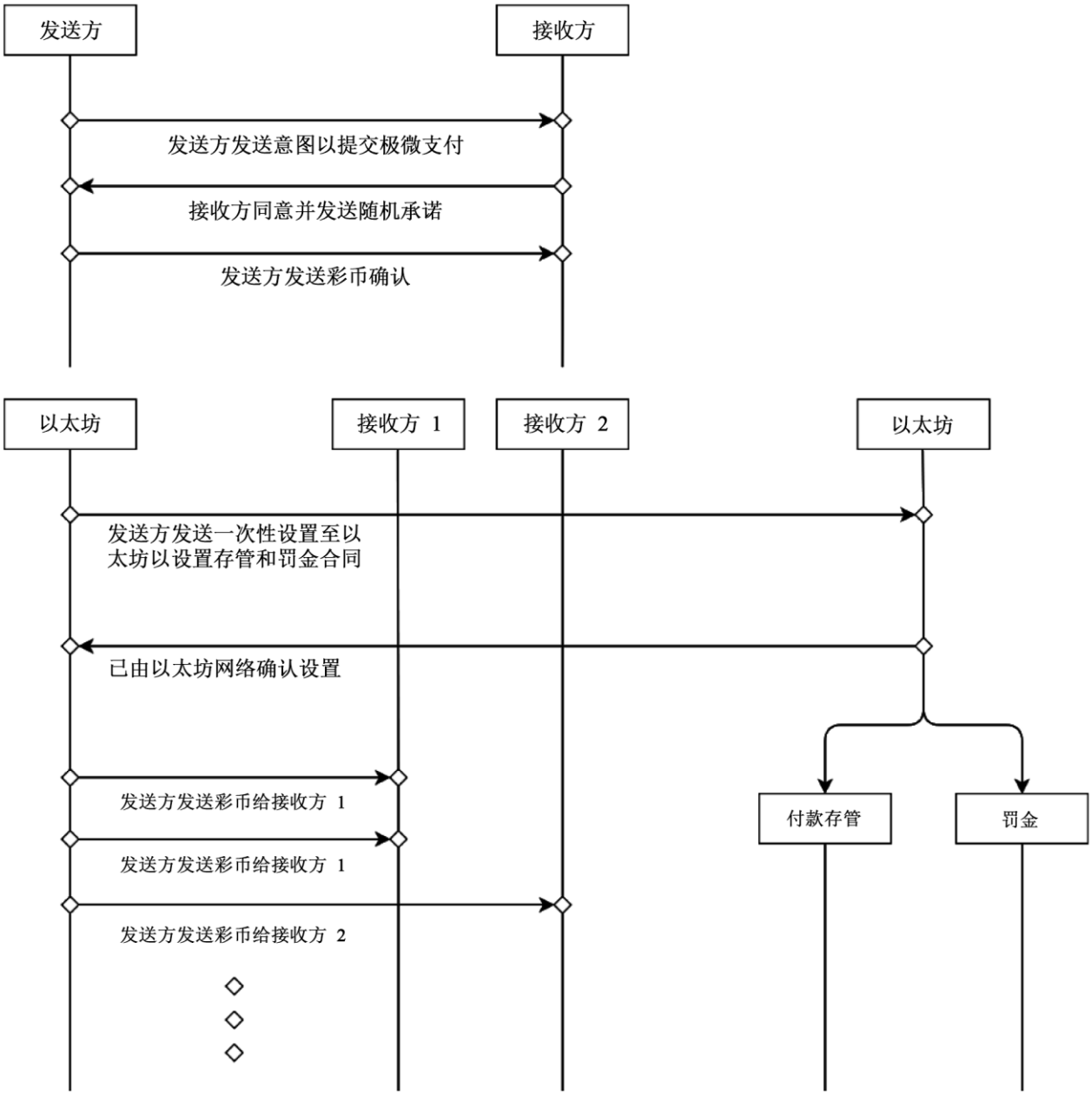
过程：

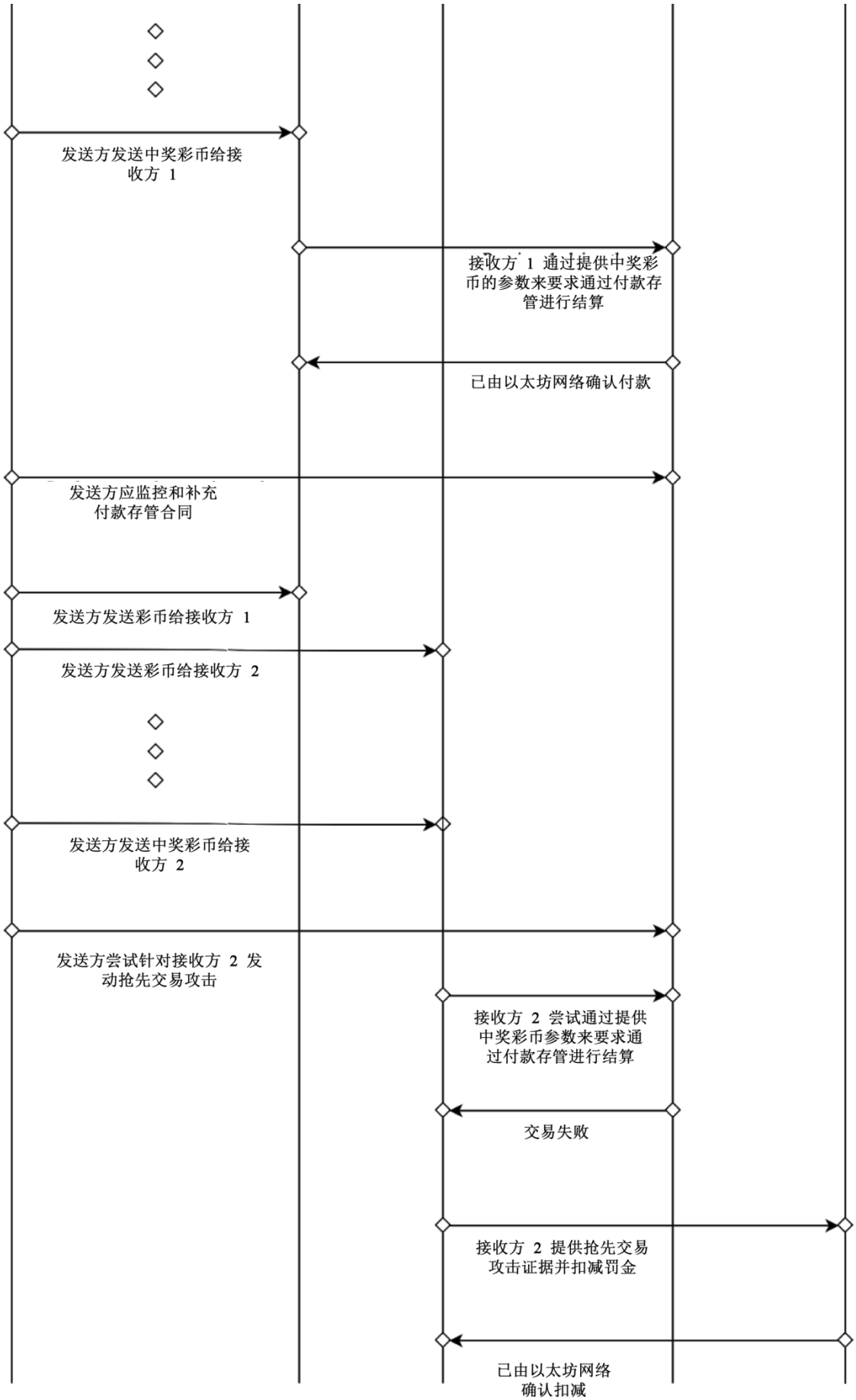
彩币生成/发送：通过交互过程“发送”彩币（或更准确地说，生成彩币）的过程。首先，接收方向发送方发送一个随机承诺，以开始随机数生成过程。然后，发送方将包含剩余信息的彩币发回，供接收方生成彩币，其中包括发送方的随机数。

结算/兑换：兑换、结算或兑现中奖彩币的过程。首先，通过让接收方签署收到的信息来生成中奖彩币，并将其广播到以太坊网络。然后，付款合约从付款余额中划拨资金到接收方的地址。

下面的程序流程说明如何使用 Orchid 极微支付方案在付款方与接收方之间进行付款。

彩币生成过程


发送方
接收方
发送方发送意图以提交极微支付
接收方同意并发送随机承诺
发送方发送彩币确认
以太坊
接收方 1
接收方 2
以太坊
发送方发送一次性设置至以
太坊以设置存管和罚金合同
已由以太坊网络确认设置
发送方发送彩币给接收方 1
发送方发送彩币给接收方 1
发送方发送彩币给接收方 2
付款存管
罚金


发送方发送中奖彩币给接收方 1
接收方 1 通过提供中奖彩币的参数来要求通过付款存管进行结算
已由以太坊网络确认付款
发送方应监控和补充付款存管合同
发送方发送彩币给接收方 1
发送方发送彩币给接收方 2
发送方发送中奖彩币给接收方 2
发送方尝试针对接收方 2 发动抢先交易攻击
接收方 2 尝试通过提供中奖彩币参数来要求通过付款存管进行结算
交易失败
接收方 2 提供抢先交易攻击证据并扣减罚金
已由以太坊网络确认扣减

在该程序流程中，需要注意以下三个重要事项。首先，付款方只要进行一次设置，相比其他现有解决方案，其设置成本非常低。虽然这会带来重复支付和抢先交易等潜在问题，但在本文稍后部分，我们从数学和经验角度上证明了这几乎不可能发生。其次，每个接收方都与相同的付款第三方存管和会员合约交互，使得每个发送方/接收方对的设置成本都变得极低。此外，这意味着不需要锁定或在接收方之间分摊向不同接收方支付的资金，因此可减少锁定在缺乏流动性的第三方存管处的资金（用作付款渠道抵押）。这是由统计复用现象（在网络中极为常见）导致的。最后，所有极微支付都在链下进行，效率有保证，但它们将信任委托到链上来处理结算，最终消除了以前的概率微支付方法对第三方的依赖性。

我们在下文中对 Orchid 极微支付方案与现有的微支付方案的特点进行了比较。在以下各节和附录中，我们进一步证明上述说法的合理性。

F 表示功能齐全，P 表示有部分功能，N 表示无功能

付款方案	可扩展性	去信任性	不可审查性	匿名性
中心化	[N, P, F]	N	N	N
支付渠道	F	P	P	N**
概率微支付	F	P*	P*	N**
Orchid 极微支付	F	F	F	N**

** 受到现有实施方案的限制*

*** 可以使用混合地址、一次性地址等进行寻址。第 5.8 节进一步讨论匿名性*

n=L2 网络中的节点数

C=每个节点的平均连接数

付款方案	路由复杂度	网络设置复杂度	资金分配系数*
中心化	不适用	不适用	不适用
支付渠道	$log_C(n)$	C	$\frac{1}{C}$
概率微支付	1	C	$\frac{1}{C}$
Orchid 极微支付	1	1	1

** 表示每个对等方可以进行交易的资金占总资金的比例。通常，分数值越低，整个网络的吞吐量也越低。*

5.3.1.与 MICROPAY 的区别

虽然 Orchid 极微支付协议的通用方案与 MICROPAY[40] 类似，但在 Orchid 方案中，我们对基本假设做了一些更改，带来了一定的效率优势。此外，这些假设将使我们能够在原始方案的理念背后引入一种在理论上保持可扩展性和抗审查性的实现方式。

在 Orchid 极微支付方案中，我们更改了以下假设：

1. 原假设：每个付款第三方存管只能由一个接收方使用，以避免重复支付
    a. 更改为：每个付款第三方存管可由多个接收方用于兑换中奖彩币
2. 添加：必然有一种方法能够减少两个不同接收方造成的资金损耗
3. 原假设：使用比特币脚本
    a. 更改为：使用以太坊智能合约及其支持的基本加密功能
4. 原假设：使用相互信任的第三方处理付款第三方存管
    a. 更改为：使用基于以太坊的智能合约处理付款第三方存管

我们将在第 5.10 节中讨论这些更改对于安全性、重复支付、抢先交易等的影响。

5.4 Orchid 代币 (OXT)

Orchid 代币 (OXT) 是一种新的符合 ERC20 规范的代币，固定供应量为 10 亿个单位，标准可细分性低至 18 个小数位（与 ETH 一样）。没有通货膨胀。当采取“销毁”货币的合约惩罚机制（例如，在极微支付帐户中采用的方法）来避免重复付款（第 5.10 节）时，有可能造成少量额外的通货紧缩压力。

使用新的自定义代币作为 Orchid 市场的货币可提供使用 ETH 等通用货币无法获得的经济激励优势。更具体地说，与使用通用货币相比，要求大型提供商投入大量资金持有特定于我们市场的自定义实用货币会产生更强的激励调整效果，因为提供商的行为将更强烈地影响自定义市场代币的价格，进而影响其持仓权益。如果我们改为使用 ETH 等通用货币，这种关联将非常弱，因为 Orchid 市场的健康状况对 ETH 价格的预期影响要小得多。

5.5.Orchid 手续费成本

我们当前使用开源 Solidity 实现关键彩币兑换函数，当就中奖彩币调用该函数时，手续费约为 10 万单位，其中包括底层 ERC20 转账的成本（仅就中奖彩币调用该函数）。

5.6 抗审查性

与其他区块链加密货币协议类似，Orchid 支付协议继承了以太坊的抗审查性。在非中奖彩币常规操作期间，极微支付协议仅涉及发送方与接收方之间的直接通信。只有中奖彩币才需要接收方将交易提交到以太坊区块链上，因此 Orchid 极微支付具有与常规以太坊交易相同的抗审查性。

审查所有 Orchid 的特定以太坊交易（或特定接收方的所有 Orchid 兑换交易）将需要大多数矿工同意忽略包含这些 Orchid 交易的所有中奖区块。由于高利润风险或成本以及以太坊采矿社区的去中心化性质，我们认为这种情况几乎不可能发生。如果一部分以太坊节点拒绝在其中奖区块中包含 Orchid 交易，则可以实现有限形式的部分审查，但是这只会以 1/(1-X)（其中 X 为审查组的相对哈希算力）的比例增加交易费用。

请注意，正如*第 5.2.3 节*中对付款渠道的论述一样，日蚀攻击可能有害，特别是在付款方或接收方运行完整节点并依赖对该完整节点的信任来向网络提交交易时。但是，在使用 Orchid 的极微支付时，付款方和接收

方无需运行完整节点就能加入 Orchid 极微支付网络。此外，运行节点的任何一方还可以向其信任的对等方或知名的公共对等方提交交易，以确保其交易不受审查。这是 Orchid 方案及相关实现相对于现有 L2 支付渠道方案的主要优势之一。

5.8 匿名性

Orchid 极微支付只是伪匿名的：在兑换中奖彩币期间，接收方将通常私有的离线客户端/服务器付款信息发布到链上，从而创建永久的公开记录。因为不发布未中奖彩币，所以未中奖彩币的付款信息仅会向收款方透露。这可减少支付信息的泄露，但在使用数周到数个月之后，中奖彩币仍会累积并留下一条公开信息轨迹，将用户的帐户公钥与他们付过款的某些 Orchid 提供商关联起来。支付彩币不会透漏该客户端连接到的特定服务器，而仅透漏提供商的公钥，但是较为老练的攻击者可能会冒充用户建立任何服务器的公钥和物理地址的模型。

对于大多数用户来说，如此少量的信息泄露并非什么严重问题；需要更强的支付隐私性的用户可以采取适当措施，切断其以太坊帐户与现实世界身份之间的联系，然后再向其极微支付帐户注入资金（使用混合服务、转换为匿名加密货币等）。对于多跳路由，Orchid 客户可以对回路中的每个节点使用单独的极微支付帐户和公钥，以防止从链上付款历史记录推断出路由（假设事先已适当地剥离了多个注资帐户）。

5.9 可扩展性分析

Orchid 极微支付系统是一种第 2 层扩展解决方案，可提供比现有第 1 层区块链支付系统高多个数量级的交易吞吐量，但最终最大可行交易吞吐量是底层第 1 层基础的数倍。在我们的极微支付系统中，链上交易有以下三个主要来源：

1. 用户向/从极微支付帐户存款/取款
2. 销售商向/从质押注册表帐户质押保证金/撤回
3. 销售商兑换中奖彩币

我们将首先从交易费用的角度评估可扩展性，然后从以太坊的基本交易吞吐量限制的角度评估可扩展性。

对于手续费成本为 2 万单位左右的标准交易，典型的以太坊平均交易费用约为 0.05 美元 [51]。典型的 VPN 用户会预付 6 个月至 1 年或更长时间，因此，我们假设大多数 Orchid 用户通常会通过在其极微支付帐户中存入 10 到 50 美元来“预付”资金，以出资购买数月的带宽。因此，即使假设手续费成本较高，用户存款和取款的交易费用也只是很小的开销。带宽销售商质押保证金/撤回的交易费用甚至更低：如果典型的销售商至少有数千个客户，每月收入超过 1000 美元，并且每月仅增加或减少一次质押，则交易费用开销将少于 0.1%。

彩币兑换交易成本的开销有所不同。极微支付的期望值是中奖概率乘以面值，从而可以灵活地在波动和交易费用之间进行折衷。使用较低的中奖概率和较高的面值，可以通过降低单位时间中奖彩币的预期数量来降低交易费用成本，但代价是会增大波动。相反，高中奖概率、低面值的彩币可减小波动，但会导致中奖人数、兑换次数和交易费用增多。

当前的 Orchid 智能合约支付兑换函数使用约 10 万单位的手续费，相当于 0.02 美元至 0.20 美元的交易费用（反映当前价格）。使用“合理的交易费用开销为 5%”这一假设，可得出彩币面值为 4 美元。如果用户在其

极微支付帐户中存入 40 美元来获得 4 个月的带宽使用权，则在这 4 个月的时间里，平均将发行 10 个中奖彩币。

我们可以使用二项分布来模拟该余额的耗尽速度。假设彩币以大约每秒 1 个的摊销率发行（该使用模式不是分析的基本特征，仅用于说明目的）或在 4 个月的时间里发行约 1000 万个，中奖率为 10^{-6}。如果有 10 个中奖者，则该帐户在 2 个月或更短的时间内耗尽余额的可能性约为 1.8%，即比预期速度快两倍以上。相反，该帐户将持续 8 个月或更长时间的可能性只有约 0.6%。

要最大限度减少本示例中的交易费用，我们可以将中奖率降低为十分之一，并使用面值为 40 美元的彩币，这样做的预期结果是 4 个月里仅发行 1 个中奖彩币。这可将交易费用开销降低至 0.4%。但是，采用该设置时，耗尽余额的风险极大：现在，在 2 个月或更短的时间内耗尽帐户余额的几率约为 30%。

以太坊区块链中的交易吞吐量取决于交易手续费成本（交易的已编译 EVM 代码的固定属性）以及区块手续费限制和区块生产率（这两者都是随时间变化的）。我们的彩币索款函数的手续费约为 10 万单位。以太坊目前支持每区块 1000 万单位的手续费[52]，生成速率为每 13 秒一个区块[53]，10 万笔手续费交易将带来约 7 tps 的吞吐量（即每月 1800 万笔交易）。假设以太坊仅用于 Orchid 交易，则使用之前的示例（每用户每月约 2.5 个中奖彩币）将使用户扩展上限达到约 700 万。

要将 Orchid 的极微支付系统扩展到数千万甚至更多的用户，将需要在下面的第 1 层区块链中部署和进行扩展性改进，例如具有分片的以太坊 2.0，或迁移到具有更高基本吞吐量的新的第 1 层解决方案。

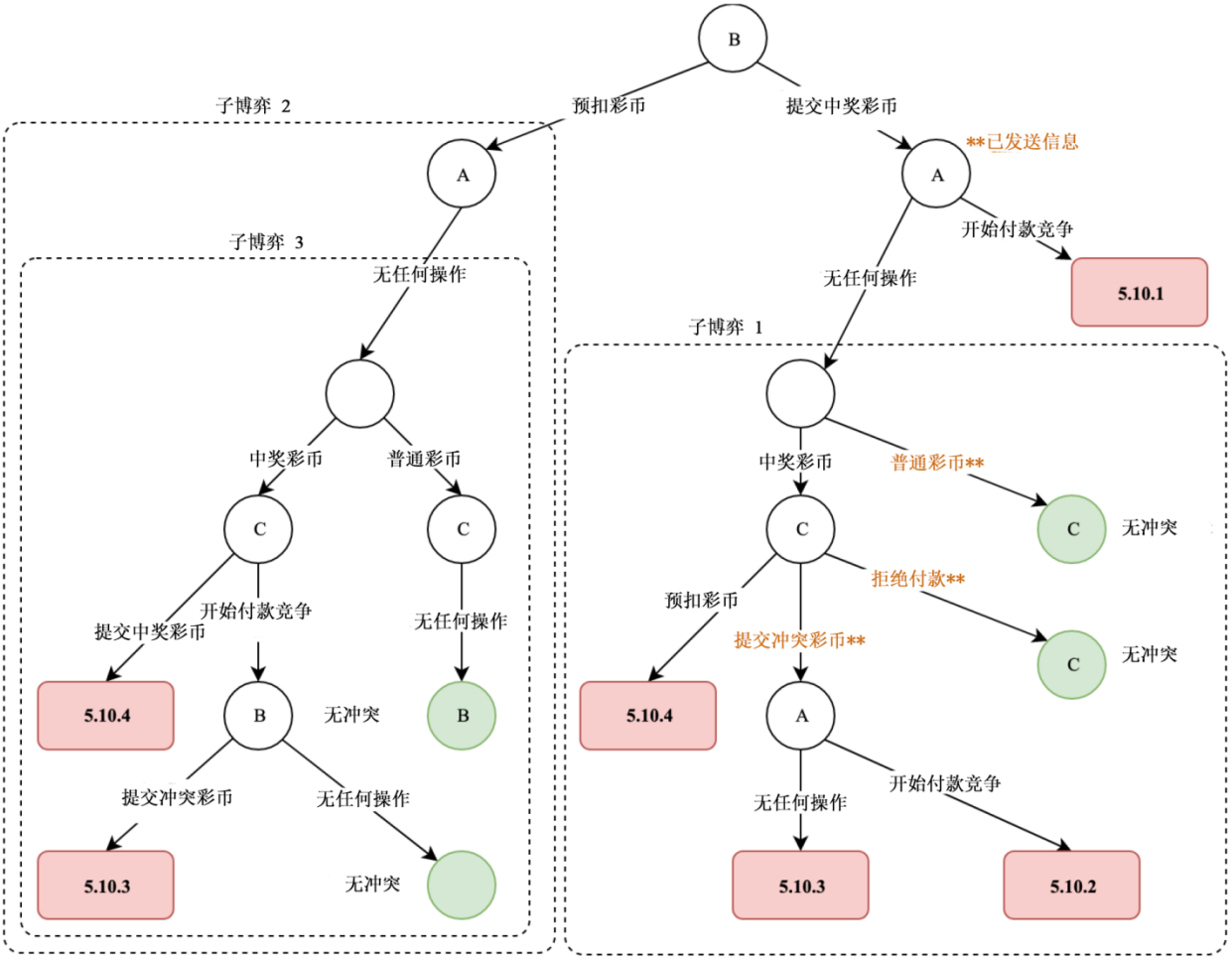
5.10 防止恶意破坏的加密经济学方法

如*第 5.3.1 节*中所述，现有的概率微支付方案与 Orchid 极微支付之间的主要区别之一是是否需要采用加密经济激励措施来防止恶意攻击。这是因为特定付款方 *A* 向其发送极微支付的每个接收方都从相同的付款智能合约（属于 *A*）兑换中奖彩币。我们在*第 5.3 节*中讨论产生的效率影响。

该设计带来的最大问题的核心在于：接收方收到来自付款方的中奖彩币，但由于付款第三方存管中的资金不足而无法结算。当付款第三方存管中的余额不足以支付将提交的所有中奖彩币时，显然会发生这种情况。我们在下面绘制了广义博弈树，概述了可能会发生哪些不同的攻击案例。我们指定以下假设：

1. 我们使用广义博弈树的目标不是找到最佳策略，而是避免不良策略
2. 从网络治理的角度来看，“不良”策略是导致无法全额支付合法中奖彩币的任何策略
3. 因此，我们并未绘制导致合法支付的所有策略，而是着重于可能导致不良策略的行为
4. 对于行为者是恶意还是良性、遵守还是背离协议，我们不做任何假设
5. 我们取最小假设，即“当攻击成本高于预期净收益时，理性行为者不会选择攻击”

不管有没有上述假设，我们的目标都是找到潜在的不良策略，并引入激励模型来避免这些不良策略。我们假设行为者仅在付款第三方存管有充足资金支付中奖彩币时采取行动，则任何人都没有理由使用这一无法正常运作的付款系统；若假设不成立，则对付款方和接收方的激励和抑制措施都会失效。我们在下面绘制了广义博弈树的简化版本。虽然对该树做了简化，但我们将证明该树的其他分支都将归入*第 5.10.5 节*的图中列出的四种失效案例。



A = 付款方　　*B、C = 接收方*

我们可以看到，Orchid 极微支付方案的参与者可以采取的许多步骤都会导致不良策略。接下来，我们将对每一种案例进行分析，以说明我们可以如何通过针对每种子案例的局部激励措施来防止出现这种不良策略。

注意，在 B 提交中奖彩币之后“发送的信息”指的是 B 有中奖彩币这一信息向网络的传播。虽然接收该信息本身并非一项决策，但有许多决策取决于是否存在该信息。特别是，*子博弈 1* 顶部的随机节点正在生成发送给 C 的付款 - 知道 B 有中奖彩币的诚实节点 C 会立即拒绝来自 A 的所有付款。这是 Orchid 实现的功能 - 如果知道有针对 A 的付款的现有索偿，则应拒绝所有其他数据包。虽然这是我们实现的功能，但我们注意到，即使良性（或恶意）行为者未遵循该规则，或尚未收到 B 有中奖彩币的信息，以下漏洞分析仍可提供抵御不良策略的加密经济学激励措施。

5.10.1 付款方单实体抢先交易攻击

这种攻击通常称为抢先交易攻击，发生在付款方尝试在 B 能够结算之前向付款第三方存管提交中奖彩币来避免结算，从而避免向 B 付款的情况。抑制这种攻击的关键在于确保因尝试抢先交易而收到的罚款高于抢先交易所能获得的收益。我们在下面列出了定义。

B_{Escrow} = *付款第三方存管余额*
$B_{Membership}$ = *会员余额*
V_{Ticket} = *彩币面值*

r_{win} = *彩币中奖率*
V_{txn} = *交易成本*
V_{Ticket} - V_{txn} = *彩币结算价值*

对于抢先交易攻击，我们的目标是通过充分抑制付款方的收益，使其在理性情况下不会选择进行此种攻击，从而减少不良策略的出现。特别是，必须让执行此种攻击的付款方付出*高于* 直接支付彩币的成本。换句话说，付款方从进行此种攻击获得的收益必须*少于*直接支付彩币的收益。

$$V_{Ticket} - V_{txn} < B_{Membership} - V_{txn}$$

只要上面的不等式成立，而这很容易在链上指明和验证，就可以通过削减会员存款来抑制理性付款方选择第二种情况，从而使得执行不良策略的代价高于直接付款给接收方。

5.10.2 付款方多实体抢先交易攻击

当多个接收方快速连续收到中奖彩币时，其中一些可能会在他们中的任何一个尚不知道其他人也在向付款第三方存管索款前就开始结算。在这种情况下，付款方可能会进行抢先交易攻击，甚至还可避开上面的不等式。如果快速连续提交了 n 个中奖彩币，则上述阻止多实体抢先交易攻击的不等式将变为：

$$Payout = n * (V_{Ticket} - V_{txn}) < B_{Membership} - V_{txn}$$

遗憾的是，要保持该不等式成立，必须解决以下两个问题。首先，如果 n 不受限制，则必须在罚金余额中锁定的代币数量将开始随接收方数量和支付规模线性增长，这使得 Orchid 极微支付方案的资金分配效率不再优于其他付款方式。其次，它增加了完全良性的中奖彩币冲突所造成的潜在损害（详见*第 5.10.3 节*）。因此，似乎没有什么符合逻辑的方法能够既不违反我们的系统设计假设，又不引入抑制良好行为的激励措施。幸运的是，只要我们引入一个稍微强一点的假设，就可以解决这个难题。

我们假设，如果理性行为者从实施不良策略中获得的效用的期望值低于其他策略，则其不会选择不良策略。基于这一假设，我们可以限制系统可能承担的风险，并确保抢先交易攻击的预期成本较低，以最大限度减少锁定资金。然后，我们可以根据该限制将缩小 $B_{Membership}$ 的范围。为此，我们引入以下假设以及其他定义：

Δ = *A 提交中奖彩币结算与 B 得知这一情况的平均时间差*
r_{OXT} = *付款方发送给接收方的 OXT 每秒摊销率*
$V\Delta$ = *付款方与接收方之间随时间 Δ 转移的 OXT 的价值*
$N\Delta$ = *付款方与接收方之间随时间 Δ 发送的彩币数量*
r_{Ticket} = *E（每秒中奖彩币数量）*

根据定义，我们可以推导出：

$$V_\Delta = r_{OXT} * \Delta$$

$$N_\Delta = \frac{V_\Delta}{Expected\ Value\ of\ Ticket} = \frac{V_\Delta}{V_{Ticket} * r_{win}}$$

$$r_{Ticket} = \frac{r_{OXT}}{V_{Ticket}}$$

要获得有 n 个总付款对等方时发生中奖彩币冲突的可能性（其中 W=*找到一张中奖彩币*），我们进行以下计算：

$$P(c\ collisions|W) = C_c^{n-1} P(\ specific\ Receiver\ collision|W)^c P(specific\ Receiver\ no\ collision|W)^{n-c-1}$$

$$P(specific\ Receiver\ no\ collision|W) = P(not\ a\ Winning\ Ticket)^{N_\Delta} = (1 - r_{win})^{N_\Delta}$$

这意味着，随着中奖率 r_{win} 的下降，发生冲突的可能性也会降低。因此，为避免冲突，直观的付款超参数选择方法是降低中奖率。我们看看如何用这种方法限制会员余额：

$$P(specific\ Receiver\ collision|W) = 1 - P(specific\ Receiver\ no\ collision|W) \approx 1 - e^{(\frac{-r_{OXT} * \Delta}{V_{Ticket}})}\ if\ r_{win} \ll 1$$

$$P(c\ collisions|W) \approx C_c^{n-1}(1 - e^{(\frac{-r_{OXT} * \Delta}{V_{Ticket}})})^c (e^{(\frac{-r_{OXT} * \Delta}{V_{Ticket}})})^{n-c-1}$$

根据前面得到的冲突可能性，我们可以计算出抢先交易攻击导致的预期损失的范围：

$$E(payout) \approx V_{Ticket} + \sum_{i=1}^{n-1} (P(i\ collisions|W) * i * V_{Ticket})$$

$$E(payout) \approx V_{Ticket} + \sum_{i=1}^{n-1} (C_i^{n-1}(1 - e^{(\frac{-r_{OXT} * \Delta}{V_{Ticket}})})^i (e^{(\frac{-r_{OXT} * \Delta}{V_{Ticket}})})^{n-i-1} * i * V_{Ticket})$$

只要满足 $E(payout) < B_{Membership}$，则一般而言，尝试进行抢先交易攻击就没有益处。为了最大限度减小 $E(payout)$，从而减少必须锁定的资金额度，同时保持针对不良策略的加密经济学抑制措施，此处也可以应用上面的超参数策略。我们只需选择一个较大的 V_{Ticket}，并相应地选择一个较小的 r_{win}。因此，上述选择付款超参数的直观方法（直接降低彩币中奖率）有效地为锁定在会员余额中的资金提供了一个可证明的界限（会员余额可以降低，以相对于接收方的数量实际上保持不变）。

但请注意，该模型不影响付款方有效监视许多接收方（如果不是所有接收方）的能力。如果这是可能的，则付款方在无利可图的情况下可能不会尝试抢先交易攻击。作为一项应对措施，上面的超参数策略已使发生这些情况的可能性大幅下降：随着冲突可能性的逐渐减小，预期的冲突成本也将逐渐减小，因此可以忽略不计。

下面，我们给出了不良和良好付款超参数的一些经验性选择，以及与其对应的冲突率。注意，即使只发生一次冲突，我们也将测量其冲突率。本节中的分析主要是为了保护接收方免受抢先交易攻击，这意味着在本节的上下文中，是否仅接受符合安全参数的付款由接收方决定

参数	Δ	r_{OXT}	r_{win}	V_{Ticket}	冲突率 $n = 2$	冲突率 $n = 10$	冲突率 $n = 100$
不良策略	300 秒	$3 * 10^{-6} \frac{OXT}{s}$	10^{-2}	$0.12\ OXT$	$\sim 0.747\%$	$\sim 6.527\%$	$\sim 52.41\%$

一般策略	30 秒	3 $*10^{-6}\frac{OXT}{s}$	10^{-3}	1.2 OXT	~ 0.007	~ 0.067	~ 0.740%
良好策略	3 秒	3 $*10^{-6}\frac{OXT}{s}$	10^{-4}	12 OXT	~ 0.000	~ 0.000	~ 0.00742

5.10.3 多实体付款争用

多实体付款争用指的是中奖彩币冲突，这并非针对付款方的恶意行为。付款争用是自然而然发生的。但是，导致付款争用的情况有两种 - 一是在*子博弈 1* 中概述的情况，二是*子博弈 2* 所述的情况。下面，我们简要介绍这两种情况，并讨论如何进行预防。

子博弈 1：意外付款争用

当发生意外付款争用时，我们可以使用*第 5.10.2 节* 中的冲突分析来选择可最大限度避免意外付款争用的超参数。虽然在异步设置中不可能完全避免付款争用，但与之相关的风险如下：

$$P(Any\ collision\ per\ second|W) = r_{Ticket} * P(Any\ collision\ |\ W)$$

$$P(Any\ collision\ per\ second|W) = \frac{r_{OXT}}{V_{Ticket}}(1 - P(0\ collision\ |\ W))\ .$$

$P(Any\ collision\ per\ second|W) = \frac{r_{OXT}}{V_{Ticket}}(1 - C_0^{n-1}(1 - e^{(\frac{-r_{OXT}*\Delta}{V_{Ticket}})})^0(e^{(\frac{-r_{OXT}*\Delta}{V_{XTicket}})})^{n-1})$。

$$P(Any\ collision\ per\ second|W) = \frac{r_{OXT}}{V_{Ticket}}(1 - (e^{(\frac{-r_{OXT}*\Delta}{V_{Ticket}})})^{n-1})\ .$$

$$E(penalty|W)\ per\ second = P(Collision\ per\ second|W) * B_{Membership}$$

$$E(penalty|W)\ per\ second = \frac{r_{OXT}}{V_{Ticket}}(1 - (e^{(\frac{-r_{OXT}*\Delta}{V_{Ticket}})})^{n-1}) * B_{Membership}$$

下面的几个示例显示了付款方蒙受意外付款争用损失的风险。我们根据*第 5.10.2 节* 中的界限计算 $B_{Membership}$。

参数	Δ	r_{OXT}	r_{win}	V_{Ticket}	每秒付款争用罚金 $n = 2$	每秒付款争用罚金 $n = 10$	每秒付款争用罚金 $n = 100$
不良策略	300 秒	$3 * 10^{-6} \frac{OXT}{s}$	10^{-2}	$0.12\ OXT$	$2.258 * 10^{-8} \frac{OXT}{s}$	$2.089 * 10^{-7} \frac{OXT}{s}$	$2.735 * 10^{-6} \frac{OXT}{s}$
一般策略	30 秒	$3 * 10^{-6} \frac{OXT}{s}$	10^{-3}	$1.2\ OXT$	$2.251 * 10^{-10} \frac{OXT}{s}$	$2.026 * 10^{-9} \frac{OXT}{s}$	$2.236 * 10^{-8} \frac{OXT}{s}$
良好策略	3 秒	$3 * 10^{-6} \frac{OXT}{s}$	10^{-4}	$12\ OXT$	$2.250 * 10^{-12} \frac{OXT}{s}$	$2.025 * 10^{-11} \frac{OXT}{s}$	$2.228 * 10^{-10} \frac{OXT}{s}$

可以看到，上一节中的冲突分析主要是为了保护接收方不受抢先交易的影响，结果得到了由接收方驱动的激励措施，激励选择良好的超参数策略。请注意，在意外付款争用中，付款方会因其无法控制的争用遭受错误地惩罚。在上述最坏情况下，由于不适当的超参数选择，可能会被收取约 1% 的费用。如果是良好的策略，这笔费用可小到忽略不计。因此，意外付款争用的存在也创造了由付款方驱动的激励机制，激励选择良好的超参数策略。

子博弈 2：接收方持留攻击

如果接收方持留中奖彩币，并在另一接收方提交中奖彩币后立即进行广播，则该接收方可以对付款方实施强行削减，从而造成一种对付款方有害的不良策略。因此，我们的目标是充分抑制持留收益，以使接收方避免这种做法。请回想一下，在*第 5.10.1 节* 中，我们曾证明为了抑制单实体抢先交易行为，必须保持不变式 $V_{Ticket} < B_{Membership}$ 成立。因此，如果接收方想要防止恶意破坏，则在初步检查时，造成损害的金额要高于造成损害的成本。一种解决方案是随时间流逝减少烧毁的金额。但是，这会开始干扰上述阻止付款方发起的攻击媒介的密码经济学不变式。

因此，我们的下一个最佳行动方案是尝试减少潜在持留方可能造成的损害。请注意，上述分析让我们能够计算发现中奖彩币后的冲突可能性！换句话说，如果我们仅认为中奖彩币在上述持续时间 Δ 内有效，则随时间推移，付款争用罚金将与*子博弈 2* 相同（有关经验性分析，请参阅上文）。请注意，不仅持留攻击的预期损失率将逐渐减小，损害本身也仅在持续时间 Δ 内有效。该有效期是可变的，实际上可能会比执行索款的预期时间短，从而进一步降低了造成损害的几率。

因此，当选择了良好的参数时，持留攻击的预期损失会小到难以察觉。由于预期损失非常小，攻击者的预期成本与受害者的预期损失的比率极高，根据我们的理性攻击者模型，这可以防止因持留攻击而出现不良策略。如*子博弈 1* 中所述，这进一步创建了由付款方驱动的激励机制，鼓励选择良好的超参数策略。

5.10.4 持留

请注意，从理性角度看，这对于任何良性或诚实的接收方来说都不是有效的策略。他们因持留行为获得的预期实际收益极小，而最糟糕的是，他们却要因此放弃中奖彩币以及与之相关的付款。事实上，对于持留，我们只关心两种情况：进入递归子博弈中的持留下降和持留攻击。所有其他情况对网络都是良性的，没有机会造成不良策略 - 实际上，持留只会对持有人造成直接经济损害。因此，如 5.10.3 子博弈 2 中所述，我

们只需要让所有中奖彩币包含一个到期时间，将持留的预期损失保持在较低水平，就能激励接收方尽快结算其中奖彩币。

5.10.5 递归子博弈

本节中的广义博弈不限制行为者的数量，也不限制可以发生的行为的数量。但是，我们可以发现，上面的每种失效案例要么将违背该广义博弈的基本假设（付款第三方存管有足够的资金支付一个中奖彩币），从而逸出博弈框架，要么将递归进入子博弈 1 或 2。我们在下面枚举了这种映射。

- 5.10.2 违背基本假设。如果网络的其余部分尚未得出该结论，则对于任意接收方 B 和 C，节点 5.10.2 都将导向子博弈 1 和子博弈 3 的入口节点。
- 5.10.3 同样违背基本假设。如果网络的其余部分尚未得出该结论，则对于任意接收方 B 和 C，节点 5.10.3 都将导向子博弈 1 和子博弈 3 的入口节点。
- 5.10.4 导向子博弈 2 的入口节点

请注意，子博弈中的每个失效案例都可能导致现有博弈树的递归案例。任何良性路径（绿色节点）都可能通过递归进入任何子博弈（任意行为者收到新彩币）来引发其他潜在攻击。但是，这些子博弈将始终最终导致（当前不可行）不良策略，或在良性路径上终结。

5.10.6 总结

综上所述，基于上面的加密经济学模型，现在我们有一系列的条件和局部策略，可防止全局性的不良策略发挥作用。特别是，我们可以看到，在上述每一个攻击者/受害者案例中，都有一组可在付款前达成共识的超参数能够阻止理性攻击者实施不良策略。实际上，如果选择了适当的超参数，即使是非理性的攻击者也无法对网络展开合理的攻击，因为在适当的超参数集中，所有潜在攻击都只能造成趋近于零的破坏。在所有以利润为导向或良性行为者的案例中，激励措施将促使这些行为者就最大限度减少随机性负面影响的超参数达成共识。不管是在良性行为者假设下，还是在敌对假设下，每个参与者的局部激励措施都将自然而然地阻止不良策略的实施。

6. 攻击与防御

在本节中，我们评估特定的用例，总结相关攻击者可能采用的主要攻击方式，并分析我们的设计抵御这些攻击的能力。

6.1 威胁模型

我们可以将攻击者的主要目标划分为以下几个（非排他性）类别：

- *流量确认*：攻击者试图确认用户 A 是否正在与目标 B 通信，其中 A 为某个已知用户，B 为某个已知目标实体（例如网站）。
- *流量分析*：攻击者试图了解正在与目标 B* 通信的所有或部分用户 A*，以及相关的元数据。
- *流量阻塞*：攻击者试图阻止一组用户 A* 与一组目标 B* 之间的连接。
- *内容修改*：攻击者试图公开或秘密地修改一组用户 A* 与目标 B* 之间的通信流的内容。

我们假设有限的本地活跃攻击者具有以下某些能力组合：

- *观察*：被动地观察部分网络流量
- *渗透*：控制一部分 Orchid、以太坊节点或外部服务器

- *操纵*：主动修改部分网络流量
- *推断*：对收集的数据应用计算，以推断*未观察到的*有用信息

Orchid 无法抵御强大到有能力观察或修改所有流量或节点的全局攻击者。我们假设的是这样一种经济模型：攻击者的能力实际上受到成本的限制，而成本主要是随用户规模扩展的。

流量分析（推断）攻击

关于对匿名系统（特别是 Tor）的推断攻击，存在大量研究，我们可以将其划分为以下几个主要类别：

在*被动流相关性*方面，攻击者对网络上的一个或多个点（通常在入口和出口位置）处的流量进行观察，然后使用统计推断分析通过多跳回路的流的关系[54,55][56,57]。深度学习领域的最新进展提高了此类攻击的成本效益[54]。

利用*活动流相关性*，攻击者还可以操纵流量（例如，插入计时延迟）创建水印图案，从而大幅提高查准率和查全率[58–60]。此类攻击需要在流入口处控制硬件以注入流量水印。

在低延迟中继中，也可能出现*侧信道相关性攻击*：对一个流进行计时测量也可能获得足够的信息来了解与通过同一中继的未观察到的流的相关性[61][62]。此类攻击有可能揭示回路的可能节点，但通常不足以追溯整个回路从而获得用户的 IP。

*网站指纹识别攻击*允许攻击者仅观察连接的出口点，即可根据针对特定网站的已知指纹库的匹配流量模式，了解通过该回路的流的相关性[63],[64]。深度学习技术可自动生成这些指纹 [65–67]。网站指纹识别攻击是否仍具有足够的查准率/查全率而被攻击者实际采用还值得商榷[68]。

范围

考虑到可能的攻击者目标、能力和预算的广泛性，针对所有或广大攻击者进行常规防御超出了 Orchid 这样的低延迟、高带宽覆盖网络的范围[26]。因此，我们将专注于一些最常见的*经济相关*的用例及其隐含的攻击者模型。

6.2 绕过地理内容限制

当今，VPN 最常见的用例之一是绕过对 Web 内容的地理限制[20]。Netflix 等流媒体服务通过从用户 IP 地址推断用户的位置，然后针对该特定位置限制对自定义库的内容访问，来实施地理许可限制。

在该用例中，攻击者的目标是修改内容和控制目标网站本身，这带来了一些有趣的挑战。攻击者很容易就可以通过 IP 地址检测最常见的 VPN 或代理服务，然后完全阻止网站访问[21]。攻击者可以利用目标流量分析的基本形式，使用 IP 注册数据库查找与已知 VPN 公司关联的 IP 地址范围，或查找共享同一 IP 地址的大量不同帐户，从而确定某个特定地址很可能为代理服务器或 VPN 服务器。

[20] https://www.geosurf.com/blog/vpn-usage-statistics/
[21] https://help.netflix.com/en/node/277

当今的 VPN 可以使用多种策略为客户端提供适合逃避地理内容锁定的模糊 IP 地址。最简单但最昂贵的方法是作为一项附加服务，为每个客户端提供唯一的 IP 地址。或者，VPN 也可以快速周转 IP 地址（通过转租等方式），从而为客户端提供不断更新的未被阻止的地址。

原则上，带宽销售商可以利用 Orchid 的元数据注册表（第 4.2 节）来使用自定义标记（例如“unique_ip”）来宣传唯一的 IP 地址。然后，客户端可以根据此标记以及地理位置进行筛选，以找到声称在特定位置使用唯一 IP 地址的出口节点。此操作的障碍是，Orchid 市场是围绕关于快速、无状态、半匿名交易的假设而构建的，而唯一 IP 地址则需要大量的构建成本。如果用户连接到实际提供新的唯一 IP 地址的节点，然后在几秒钟后断开连接，则该用户最终将需要支付极少美元的服务费用，而提供该服务所花的费用大约比此高出一百万倍。而 Orchid 销售商可能会针对唯一的 IP 地址服务收取更高的宏支付金额；这将需要用户在客户端 UI 中明确批准大额发票，并且我们预计这仅对高度受信任的策划销售商具有可行性。

或者，销售商可以选择直接宣传解除对特定流媒体服务的阻止。这一要求的功能可否实现取决于销售商：他们可以通过轮换新的 IP 地址和较低的用户/ IP 地址比来实现解除阻止。如果成功，则销售商可以通过此项服务收取更多带宽费用，而无需提前进行宏支付。

从长远来看，Orchid 允许用户从各种不同的提供商访问服务器，避免了当前 VPN 模型固有的锁定风险，因此在此用例中具有一项关键优势。使用单个 VPN 订购时，如果特定提供商的服务器突然被阻止，用户几乎没有追偿权。而使用 Orchid，用户随时可以轻松地、几乎是即时地切换提供商。

6.3 点对点共享系统

点对点网络是用户绕过集中式内容源来直接共享内容的一种常见方式。ISP（互联网服务提供商）可能会出于各种原因而想要限制或干扰点对点共享网络：他们可能会将其视为对有线电视或流媒体收入的威胁，他们可以使用大量带宽，并且可以允许用户共享受保护的内容。威慑是攻击者的主要目标之一，首先会进行流量分析：他们希望识别正在使用特定 p2p 网络和/或共享特定内容的用户的身份。

此用例中攻击者的能力相当有限：他们的主要攻击策略是：进行检测，然后对 p2p 数据包筛选；或者，通过运行自己的节点来渗透到点对点网络中，然后由这些节点记录特定用户的 IP 地址、操作和元数据。当前常见的点对点网络（例如 Bittorrent）能够以较低成本实现安全性；渗透这些网络的费用也不高。VPN 通过为流量加密和简单地隐藏用户 IP 地址这两种方法，在许多辖区为这种用例提供充分的保护。只要 VPN 在法律或财务上均没有保存日志的义务，或者攻击者难以获取日志，则这种做法便是可行的。

通过将权益加权选择机制和白名单相结合，Orchid 可为此用例提供类似于 VPN 的强大防御能力。如果某 Orchid 客户端使用的白名单仅包含已知可帮助避免日志记录的受信任提供商，则该客户端避免节点和攻击者共谋的概率相似或更高，这是因为用户从已知可帮助避免日志记录的 VPN 列表中随机选择 VPN。

如果用户同时选择了攻击者控制的 Orchid 节点和 p2p 文件共享网络（例如 Bittorrent）节点，则攻击者可以成功完成此攻击。概率的计算公式如下：

$$p(compromise(x,y): x \in A_o, y \in A_B) = p(x \in A_o)\, p(y \in A_B) \quad (20)$$

$$p(y \in A_O) = \frac{S_{A \cap W}}{S_W} \quad (21)$$

$$p(y \in A_B) = \frac{B_A}{B_T} \quad (22)$$

x, y：分别是选定的 Orchid 节点和文件共享节点

A_o,A_B：节点集，其中所含的 Orchid 节点和文件共享节点由攻击者分别控制

W：客户的白名单，即一组 Orchid 节点

S, S_W:分别是 OXT 总权益和 W 中节点的 OXT 权益

$S_{A \cap W}$: $A \cap W$ 中节点的 OXT 总权益，也位于 W 中的攻击者节点集

B_A,B_T：分别是文件共享网络上的攻击者带宽和总带宽

如果没有白名单 W，则 S_W 等于系统总权益 S_T，而选择攻击性 Orchid 节点的概率仅为 $\frac{S_A}{S_T}$，即攻击者控制的所有 OXT 权益中的相对部分。假设 Orchid 有几百万个用户，且 Orchid 总权益价值约为 10 亿美元（第 4.4 节），那么，与向未受保护的用户发动攻击相比，针对 Orchid 节点制定了 1000 万美元预算的攻击者向单跳 Orchid 用户发动攻击的成功率要低三个数量级。对于任何连接到攻击者控制的文件共享节点的 Orchid 用户而言，同时连接到攻击者的其中一个 Orchid 节点的概率仅为 0.1%。

随机白名单无效，这是因为在这种情况下，$\frac{S_{A \cap W}}{S_W} = \frac{S_A}{S}$。相比 S_W，精心选择的白名单可将 $S_{A \cap W}$ 减少的幅度要大很多，并且可以大幅降低破坏概率。

假设攻击者没有能力进行有效的流量时间分析攻击，则多跳线路可以大幅降低选择概率：

$$p(compromise(X_k)) = \left(\frac{S_{A \cap W}}{S_W}\right)^{\lceil k/2 \rceil} \frac{B_A}{B_T} \quad (23)$$

此处的 X_k 代表 k 跳线路；攻击者必须控制此线路中的所有其他节点才能推断出完整路径。对于典型的 3 跳线路，攻击者必须控制 2 个特定节点：第一个和最后一个。如果在没有白名单的情况下使用与上面相同的参数，则连接到攻击者文件共享节点的用户也使用受感染 3 跳线路的概率现在仅为 10^{-6}。

高级攻击者可以使用主动流关联分析来降低多跳线路的有效性。通过将时间指纹模式注入业务流并在端点处对其进行检测，理论上，攻击者仅通过控制第一个 Orchid 入口节点和端点（在这种情况下为文件共享节点）即可关联甚至破坏冗长的线路[23- 25]。Orchid 客户端可以通过选择使用*带宽燃烧*来帮助防御以下攻击：用虚拟数据包填充数据包流以模拟连续的低差异流，以尝试擦除可检测的时间信号。

但是，在此用例中，我们认为不太可能发生这些高级流量分析攻击。这类攻击者针对每位用户的预算都非常有限。流量分析技术提供了对于监视很有用的统计关联证据，但误报率通常很高。

6.4 避免 ISP 审查

现在，许多国家/地区会审查通常由本地 ISP（互联网服务提供商）实施的、在政治上令人反感的互联网内容[69]。各个国家/地区的审查范围差异很大，但我们可以将此用例大致分为两个主要类别：将会审查但允许使用 VPN 的国家/地区（例如，印度尼西亚、巴基斯坦、泰国），以及进行广泛审查并且也禁止或限制使用 VPN 的、限制性更强的国家/地区（例如，中国，俄罗斯）。

弱审查攻击者

在允许使用 VPN /代理服务的国家/地区利用 Orchid 规避互联网审查非常简单。客户端可以使用简单的地理筛选器从受限制国家/地区外部的节点中进行选择，但是实际上，这可能不必要，因为受限制国家/地区中的出口节点无论如何都不太可能收到大量流量，正因如此，出口节点往往会聚集在很少进行审查的地点。这些国家/地区的攻击者并不会投入大量资源来规避审查，因此比较“弱者”。

强审查攻击者

积极限制 VPN /代理服务的国家/地区会带来更多挑战。尤其是中国，已实施广泛的技术解决方案来进行全面的互联网监视和审查，这些监视和审查被称为“中国长城防火墙”(GFW)。中国甚至已经开始对被抓住使用 VPN 的个人处以罚款[70]。但是，外部 VPN 在中国仍然很常见[71]，而且提供商们经常玩儿猫捉老鼠的游戏。此攻击者具有很多种能力，其中三种与规避审查尤其有关：

- GFW 使用*深度数据包检查*对可能的 VPN /代理服务器一起进行检测。
- GFW 使用*主动探测*对可疑服务器进行检查[72]
- GFW 使用自动和手动过程来禁止使用与 VPN /代理服务关联的 IP 地址

Orchid 客户端使用 WebRTC 建立隧道连接，WebRTC 增添了一层混淆功能，可规避为识别一般 VPN/代理而进行了调整的深度数据包检查工具的检测。但是，如果 Orchid 在中国普及，则他们可能会采用 GFW 数据包检查系统来识别 Orchid WebRTC 流量，这需要进一步开发混淆插件。

更麻烦的是，主要 Orchid 发现过程依赖于在以太坊区块链上发布的公共节点目录（第 4.2 节）。一旦 Orchid 在中国普及到足以引起人们的注意，GFW 很可能会自动监控以太坊区块链并禁止公共目录中所有已列出 Orchid 节点的 IP 地址。

尽管存在这些障碍，但是中国公民仍然能够以限制性基层方式按原样使用 Orchid，即国外的朋友和爱好者可以运行（可能是免费的）入口节点，然后私下共享地址。支持者和慈善家可以通过沿着与秘密 Orchid 节点地址相同的私有社交渠道分配 OXT 加密货币来进一步支持这一事业。为了更好地规避 GFW 并促进 OXT 分配到中国而进行的核心设计改进是令人兴奋的未来研究方向（第 7 节）。

6.5 监视规避

互联网监视通常比互联网审查更为普及。大多数司法管辖区的 ISP 都有一些法律义务，需要遵守执法部门提出的有效监视要求，而西方主要情报机构广泛的法外监视行动现已成为一个公开的秘密。我们会将这个范围广泛的场景分为几个模型，假设攻击者具有不同的能力组合。

被动 ISP 监控

在世界上许多地方，互联网服务提供商 (ISP) 的经济上允许并且也有能力监控客户的互联网流量并记录在日志中。在某些辖区，法律要求进行日志记录以帮助进行执法调查。出于策略原因，ISP 还可能会对数据包进行分析并根据分析结果来调整流量，使某些应用程序优先于其他应用程序。他们可能会收集用户的浏览历史记录并将这一信息出售给广告商。

在这些情况下，我们假定攻击者缺乏渗透到 Orchid 网络和/或目标端点中所需的动力和能力。在这种情况下，只要连接端点也不受 ISP 的控制，单跳线路便可以规避一般非针对性流量分析监视。WebRTC 编码还将使 Orchid 流量看起来像是对粗略数据包分析工具发出的常规 Web 请求，但骗不过熟悉 Orchid 并使用更复杂的深度数据包检查技术的攻击者。

单跳线路所提供的对采用网站指纹技术的攻击者的防御较少[65–67]。多跳线路降低了这些攻击的查准率/查全率，但却不足以使这些攻击失效。我们认为这些关联技术过于昂贵，无法 *一起*采用，但它们却会给目标用户带来潜在威胁。

被动 ISP 和端点监控

在我们的下一个场景中，攻击者有能力监视端点流量，但是他们仍然无法通过其 ISP 主动调整或控制用户的入口流量。此场景对应于一个正在积极监视特定端点（例如网站）并使用流量分析来收集有关那些目标端点的用户的信息的代理。一旦攻击者找到目标用户的 IP 地址，他们接下来将使用该地址从其 ISP 获取有关该用户的其他流量日志和个人信息。

攻击者现在可以额外采用被动流关联技术[20-22]，但是我们同样假设这些技术过于昂贵，无法跨流经 ISP 的所有流量 *一起*采用。相反，攻击者的分析预算有限，并且必须针对可能用于建立关联的用户 IP 地址。

在这种情况下，假设端点连接也使用 HTTPS/SSL 加密并且用户尚未成为目标，则单跳线路仍足以规避监视。攻击者只会看到从 Orchid 节点到端点的连接，而无法轻松确定用户的 IP 地址。

正如在 *第 5.8 节* 中所讨论的，在端点处全面监控流量的攻击者可能能够将 Orchid 节点和端点之间的流量计时与该节点兑换中奖彩币相关联。彩币将显示付款人的 Orchid 极微支付地址，然后攻击者可以将其追溯回到用户。用户可以通过采取适当的步骤来使其 OXT 加密货币匿名，从而避免这种情况。

端点和 Orchid 渗透

现在，我们来看一个攻击者，该攻击者根本没有能力监视用户 ISP 中的数据，但却可以渗透到端点和/或 Orchid 网络中。对于其 ISP 不会大规模将流量记录在日志中或不与攻击者共享大量流量数据的用户而言，此模型非常务实。现在，如果无法监控从用户通向用户第一个 Orchid 节点的链路上的流量，则流量关联攻击将变得困难的多。

攻击者可以渗透到 Orchid 网络中以执行流量关联攻击。通过渗透所实现的效力取决于攻击者针对 Adversary 节点制定的预算。质押机制可确保每个用户的捕获成本相对较高，此外，随着 Orchid 赢得用户的青睐，捕获固定百分比的 Orchid 连接的成本也会按比例地增加，如 *第 4.4 节* 中所讨论。攻击者可以通过向共谋的 Orchid 节点操作员（该操作员会保留流量日志并将其提供给攻击者）请求日志来破坏线路，也可以通过直接控制 Orchid 节点来破坏线路。单个节点的破坏概率为：

$$p(compromise(x)) = p(x \subseteq \alpha) + (1 - p(x \subseteq \alpha))p(x \subseteq A) \quad (24)$$

$$p(x \subseteq \alpha) = \frac{S_{\alpha \cap W}}{S_W} \quad (25)$$

$$p(x \subseteq A) = \frac{S_{A \cap W}}{S_W} \quad (26)$$

x：随机选择的 Orchid 节点

α:为攻击者将数据记录在日志中的共谋 Orchid 节点集

A :攻击者直接控制的 Orchid 节点集

W：客户的白名单，即一组 Orchid 节点

S_W:W 中节点的 OXT 总权益

$S_{\alpha \cap W}$:$\alpha \cap W$ 中节点的 OXT 总权益，也位于 W 中的共谋攻击节点集

$S_{A \cap W}$:$A \cap W$ 中节点的 OXT 总权益，也位于 W 中的攻击者节点集

如果攻击者需要直接 IP 地址元数据以便确认链路，则对于多跳线路，他们将需要破坏每个边缘，进而破坏每个其他节点。因此，多跳线路破坏概率是单跳概率的幂函数：

$$p(compromise(X_k)) = (\frac{S_{\alpha \cap W}}{S_W} + (1 - \frac{S_{\alpha \cap W}}{S_W})\frac{S_{A \cap W}}{S_W})^{[k/2]} \quad (27)$$

除非攻击者的经济上允许进行流量分析并且统计查准率/查全率虽不理想但也可以接受，否则多跳线路可以大幅提高安全性。如果攻击者使用流关联技术（如*第 6.1 节* 中所讨论），则多跳线路提供的破坏概率与单跳线路（公式 24）更相似。

强攻击者

较强大的攻击者可能有能力在 ISP 或 AS（自治系统）级别控制数据包。即使是仅有能力监视用户 ISP 中流量的攻击者，仍然可以使用网站指纹攻击通过多跳线路将用户与网站相关联，其主要障碍是成本。客户端可以使用*带宽燃烧*在一定程度上防御这些攻击：如果按照对底层数据流不敏感的高度规则的时间表填充加密的流量流以发送大小均等的数据包，将破坏大多数流量分析技术所依赖的时间关联。如果没有这些额外的保护措施，则针对每个用户制定了大量分析预算并且具有强大的感知或推断能力的攻击者可能会击败多跳线路。我们将在下一节中讨论这些可能性，即未来工作。

7. 未来工作

Orchid 通过可扩展的链下极微支付为分散式代理服务提供了带宽市场。从这个基础着手，我们找到了许多用于改进匿名性、可用性、抗审查性和经济安全性的途径。

抗流量分析

当存在流量分析攻击时，Orchid 当前的路由设计以牺牲匿名性为代价，最大程度地减少延迟并最大限度地增加带宽。延迟、带宽和匿名性之间的利弊权衡可能十分重要[26]。需要更强匿名性的用户可以使用带宽燃烧（恒定速率传输流），此功能可以通过擦除大部分随时间变化的签名来帮助克服流量分析。为了克服各种推断攻击，除了带宽燃烧外，可能还需要进行进一步的改进[73]，并且我们会对未来工作进行全面分析。对延迟感知型路由构建进行的各项独立改进可以在相同的延迟下实现更长的线路，并通过将稀疏连接图与沿着较少活动边缘混合的较多流配合使用来改善混合效果。

支付匿名性

Orchid 的极微支付系统基于以太坊而构建，因此仅是半匿名的。因此，要求支付完全匿名的用户需要先在外部将 OXT 加密货币匿名化，然后再向极微支付帐户提供资金，这会造成可用性障碍。

另外，Orchid 极微支付和线路本身可以允许高速混合。目录服务可以改用于宣传可提供混合和/或注册混合对等节点的节点。此用例可能会加重双重支出和恶意破坏防御机制 (5.10)，因此可能需要改进对双重支出的检测和预防。

低差异极微支付

当前的 Orchid 极微支付机制具有基本的差异/开销权衡。差异的核心来源是彩币的统计独立性。通过使用互斥采币方案，可能可以消除差异。最简单的形式是，每个支付账户可能需要有一张中奖彩币。整套彩币只有一个中奖者，因此消除了差异。一种折衷方案是，互斥彩币需要使用多方熵源（而不是简单的两方熵协议）将确定彩币中奖者的时间推迟到将来。以太坊区块链本身可以用作简单的熵源，并且对于极微支付结算所需的小额交易价值而言，可能是足够安全的。但是，推迟确定中奖者将导致大量未结算的付款在途中，从而导致每笔极微支付产生额外存储成本。

流量混淆

关于流量混淆和检测的竞争研究领域的竞争一直都在进行着。流量混淆器使用一些策略，例如，随机化[74,75]、转换/模仿[76]、隧道[76,77]以及生成模型[78]。不幸的是，所有这些技术都容易受到基于机器学习的检测[27]系统（接受过以实际流量和混淆流量为例的培训）的检测。通常，更强大的混淆器需要对每字节进行更多计算。混淆问题可以归为 GAN 目标类型 [79]，其中，生成器会学习转换业务流以规避检测，同时保留可逆性或重构属性，而鉴别器会学习区分真实流和转换流。这为基于深度学习的混淆器（和检测器）打开了大门。

改进的抗审查性

Orchid 规避省/直辖市/自治区级审查的能力主要受以太坊区块链上节点的公开宣传的限制。要增强审查抵抗性，将需要某种形式的私下宣传。我们可以将其建模为一种博弈，其中带宽销售商试图向合法客户宣传不受阻止的 IP 地址，同时又对攻击者隐藏这些 IP 地址。销售商会为每个了解 IP 地址的合法客户获得一些预期的未来收益价值，但是一旦攻击者发现 IP 地址并将其阻止，则将失去任何其余的未来收益价值。对于销售商而言，可行的策略是使用会员计划，用未来收入来源的一小部分奖励宣传伙伴。这将为擅长寻找并向合法用户宣传节点地址，同时规避敌对性串通者的会员创造市场利基。

白名单保证金

我们可以通过允许将 OXT 质押到特定白名单某个节点的范围内，来扩大质押和质押加权的积极性激励调整效果。如果从该列表中删除了该节点（在提款之前），则该笔质押保证金将被没收并烧毁。此股份将变成保证金之类的东西，从而允许节点提供商通过在行为异常时将其资金置于风险之下来证明可信赖性。这一理念很简单，但是需要仔细的激励设计和验证。

我们欢迎您创建您自己的精选清单，列出创新性激励结构。

8. 致谢

Orchid 一直以来都是一个协作团队项目，我们尤其要感谢 Gustav Simonsson 和 David Salamon 的重大知识贡献（包括他们对白皮书 0.9.2 版的编写）。

参考资料

1. Dingledine R, Mathewson N, Syverson P. Tor:The Second-Generation Onion Router [互联网]。2004 年。获取地址：http://dx.doi.org/10.21236/ada465464

2. Shahbar K, Nur Zincir-Heywood A. Effects of Shared Bandwidth on Anonymity of the I2P Network Users [互联网]。2017 IEEE 安全和隐私研讨会 (SPW)。2017 年。获取地址：http://dx.doi.org/10.1109/spw.2017.19

3. Chaum D. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms [互联网]。Advances in Information Security。2003 年。p. 211–9。获取地址：http://dx.doi.org/10.1007/978-1-4615-0239-5_14

4. HashCash [互联网]。2002 年 [引自 2019 年 9 月 10 日]。获取地址：http://www.hashcash.org/hashcash.pdf

5. Bitcoin:A Peer-to-Peer Electronic Cash System [互联网]。[引自 2019 年 9 月 10 日]。获取地址：https://bitcoin.org/bitcoin.pdf

6. Orchid 0.9.2 [互联网]。2019 年 [引自 2019 年 9 月 10 日]。获取地址：https://www.orchid.com/assets/whitepaper/whitepaper.pdf

7. Stoica I, Morris R, Liben-Nowell D, Karger DR, Kaashoek MF, Dabek F, et al. Chord:a scalable peer-to-peer lookup protocol for internet applications [互联网]。Vol. 11, IEEE/ACM Transactions on Networking。2003 年。p. 17–32。获取地址：http://dx.doi.org/10.1109/tnet.2002.808407

8. Wood DD. ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER.2014 年 [引自 2019 年 9 月 11 日]；获取位置：https://pdfs.semanticscholar.org/ee5f/d86e5210b2b59f932a131fda164f030f915e.pdf

9. A Protocol for Packet Network Intercommunication [互联网]。The Best of the Best。2009 年。获取地址：http://dx.doi.org/10.1109/9780470546543.ch54

10. Fadilpa&scaron S, i&#.China “hijacked traffic” to spy on the West [互联网]。ITProPortal。ITProPortal；2018 年 [引自 2019 年 11 月 17 日]。获取地址：https://www.itproportal.com/news/china-eavesdropping-on-western-communication-for-years-research-claims/

11. Bloomberg - Are you a robot?[互联网]。[引自 2019 年 11 月 17 日]。获取地址：https://www.bloomberg.com/news/articles/2018-09-04/youtube-and-netflix-throttled-by-carriers-research-finds

12. Morran BC.House Votes To Allow Internet Service Providers To Sell, Share Your Personal Information [互联网]。Consumer Reports。[引自 2019 年 11 月 17 日]。获取地址：https://www.consumerreports.org/consumerist/house-votes-to-allow-internet-service-providers-to-sell-share-your-personal-information/

13. Net Neutrality:Caught in a web of lobbying and regulatory uncertainty [互联网]。Sustainalytics。2018 年 [引自 2019 年 11 月 17 日]。获取地址：https://www.sustainalytics.com/esg-blog/net-neutrality-caught-in-a-web-of-lobbying-and-regulatory-uncertainty/

14. Rosenberg S. Facebook’s reputation takes a hit in new survey [互联网]。Axios。2019 年 [引自 2019 年 11 月 17 日]。获取地址：https://www.axios.com/facebook-reputation-drops-axios-harris-poll-0d6c406a-4c2e-463a-af98-1748d3e0ab9a.html

15. Marks G. Facebook Usage Drops 26 Percent…And Other Small Business Tech News This Week [互联网]。Forbes。福布斯；2019 年 [引自 2019 年 11 月 17 日]。获取地址：https://www.forbes.com/sites/quickerbettertech/2019/10/27/facebook-usage-drops-26-percentand-other-small-business-tech-news-this-week/

16. Brodkin J. 50 million US homes have only one 25Mbps Internet provider or none at all [互联网]。Ars Technica。2017 年 [引自 2019 年 11 月 17 日]。获取地址：https://arstechnica.com/information-technology/2017/06/50-million-us-homes-have-only-one-25mbps-internet-provider-or-none-at-all/

17. SSH Celebrates 20 Years as Industry Standard | SSH.COM [互联网]。[引自 2019 年 11 月 17 日]。获取地址：https://www.ssh.com/press-releases/111-ssh-communications-security-celebrates-20-years-as-industry-standard

18. Fu X, Graham B, Bettati R, Zhao W. Active traffic analysis attacks and countermeasures [互联网]。2003 International Conference on Computer Networks and Mobile Computing, 2003。ICCNMC 2003。获取地址：http://dx.doi.org/10.1109/iccnmc.2003.1243024

19. Dixon C, Bragin T, Krishnamurthy A, Anderson T. Tit-for-Tat Distributed Resource Allocation。[引自 2019 年 9 月 23 日]；获取位置：http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.182.1544

20. Karakaya M, Korpeoglu I, Ulusoy Ö.Free Riding in Peer-to-Peer Networks [互联网]。Vol. 13, IEEE Internet Computing。2009 年。p. 92–8。获取地址：http://dx.doi.org/10.1109/mic.2009.33

21. Ngan T-W "johnny," Dingledine R, Wallach DS.Building Incentives into Tor [互联网]。Financial Cryptography and Data Security。2010 年。p. 238–56。获取地址：http://dx.doi.org/10.1007/978-3-642-14577-3_19

22. Androulaki E, Raykova M, Srivatsan S, Stavrou A, Bellovin SM。PAR:Payment for Anonymous Routing [互联网]。Privacy Enhancing Technologies. p.219–36。获取地址：http://dx.doi.org/10.1007/978-3-540-70630-4_14

23. Ghosh M, Richardson M, Ford B, Jansen R. A TorPath to TorCoin:Proof-of-Bandwidth Altcoins for Compensating Relays。2014 年 7 月 18 日 [引自 2019 年 9 月 23 日]；获取位置：https://apps.dtic.mil/dtic/tr/fulltext/u2/a621867.pdf

24. A Protocol for Interledger Payments [互联网]。[引自 2019 年 9 月 23 日]。获取地址：https://pdfs.semanticscholar.org/ab98/c62a7efdc5362c7f36589680597a93f3111f.pdf

25. Khosla A, Saran V, Zoghb N. Techniques for Privacy Over the Interledger。2018 年 [引自 2019 年 9 月 23 日]；获取位置：https://pdfs.semanticscholar.org/02f3/aae499723063cf9c3cc42508cae13d16aa7d.pdf

26. Das D, Meiser S, Mohammadi E, Kate A. Anonymity Trilemma:Strong Anonymity, Low Bandwidth Overhead, Low Latency - Choose Two [互联网]。2018 IEEE Symposium on Security and Privacy (SP)。2018 年。获取地址：http://dx.doi.org/10.1109/sp.2018.00011

27. Wang L, Dyer KP, Akella A, Ristenpart T, Shrimpton T. Seeing through Network-Protocol Obfuscation [互联网]。Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15。2015 年。获取地址：http://dx.doi.org/10.1145/2810103.2813715

28. Budish E. The Economic Limits of Bitcoin and the Blockchain [互联网]。2018 年。获取地址：http://dx.doi.org/10.3386/w24717

29. 网站 [互联网]。[引自 2019 年 10 月 2 日]。获取地址：https://bitinfocharts.com/comparison/ethereum-transactionfees.html

30. Bitcoin Avg. Transaction Fee chart [互联网]。BitInfoCharts。[引自 2019 年 10 月 2 日]。获取地址：https://bitinfocharts.com/

31. Khattak S, Elahi T, Simon L, Swanson CM, Murdoch SJ, Goldberg I. SoK:Making Sense of Censorship

Resistance Systems [互联网]。Vol. 2016, Proceedings on Privacy Enhancing Technologies。2016 年。p. 37–61。获取地址：http://dx.doi.org/10.1515/popets-2016-0028

32. Contributors to Wikimedia projects.ISO/IEC 7816 - Wikipedia [互联网]。Wikimedia Foundation，Inc. 2002 年 [引自 2019 年 10 月 2 日]。获取地址：https://en.wikipedia.org/wiki/ISO/IEC_7816

33. EBICS.ORG:主页 [互联网]。[引自 2019 年 10 月 2 日]。获取地址：http://www.ebics.org/home-page

34. 网站 [互联网]。[引自 2019 年 10 月 2 日]。获取地址：https://www.swift.com/

35. 网站 [互联网]。[引自 2019 年 10 月 2 日]。获取地址：https://www.swift.com/

36. 网站 [互联网]。[引自 2019 年 10 月 2 日]。获取地址：http://www.nyce.net/about

37. 网站 [互联网]。[引自 2019 年 10 月 2 日]。获取地址：http://www.investopedia.com/terms/r/reconciliation.asp

38. [无标题] [互联网]。[引自 2019 年 10 月 2 日]。获取地址：https://www.aba.com/-/media/archives/endorsed/rippleshot-state-of-card-fraud.pdf

39. Mian A, Hameed A, Khayyam M, Ahmed F, Beraldi R. Enhancing communication adaptability between payment card processing networks [互联网]。Vol. 53, IEEE Communications Magazine。2015 年。p. 58–64。获取地址：http://dx.doi.org/10.1109/mcom.2015.7060519

40. Banks and WikiLeaks.纽约时报 [互联网]。2010 年 12 月 25 日 [引自 2019 年 10 月 2 日]；获取位置：https://www.nytimes.com/2010/12/26/opinion/26sun3.html

41. What are common credit card processing fees?[互联网]。Quora。[引自 2019 年 10 月 2 日]。获取地址：https://www.quora.com/What-are-common-credit-card-processing-fees

42. 网站 [互联网]。[引自 2019 年 10 月 2 日]。获取地址：https://www.nerdwallet.com/blog/banking/wire-transfers-what-banks-charge

43. 网站 [互联网]。[引自 2019 年 10 月 2 日]。获取地址：https://www.valuepenguin.com/what-credit-card-processing-fees-costs

44. 网站 [互联网]。[引自 2019 年 10 月 2 日]。获取地址：https://www.economist.com/blogs/dailychart/2010/12/remittances

45. 网站 [互联网]。[引自 2019 年 10 月 2 日]。获取地址：https://financefeeds.com/alipay-vs-wechat-pay-vs-unionpay-important-research/

46. Joseph Poon TD.The Bitcoin Lightning Network:Scalable Off-Chain Instant Payments [互联网]。获取地址：https://lightning.network/lightning-network-paper.pdf

47. [无标题] [互联网]。[引自 2019 年 10 月 2 日]。获取地址：https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-heilman.pdf

48. Wheeler D. Transactions using bets [互联网]。Security Protocols。1997 年。p. 89–92。获取地址：http://dx.doi.org/10.1007/3-540-62494-5_7

49. Rivest RL.Peppercoin Micropayments [互联网]。Financial Cryptography。2004 年。p. 2–8。获取地址：http://dx.doi.org/10.1007/978-3-540-27809-2_2

50. Pass R, Shelat A. Micropayments for Decentralized Currencies [互联网]。Proceedings of the 22nd ACM

SIGSAC Conference on Computer and Communications Security - CCS '15。2015 年。获取地址：http://dx.doi.org/10.1145/2810103.2813713

51. Ethereum Avg. Transaction Fee chart [互联网]。BitInfoCharts。[引自 2019 年 10 月 2 日]。获取地址：https://bitinfocharts.com/

52. 网站 [互联网]。[引自 2019 年 10 月 2 日]。获取地址：https://etherscan.io/chart/gaslimit

53. 网站 [互联网]。[引自 2019 年 10 月 2 日]。获取地址：https://etherscan.io/chart/blocktime

54. Nasr M, Bahramali A, Houmansadr A. DeepCorr:Strong Flow Correlation Attacks on Tor Using Deep Learning.In:Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security。ACM；2018 年。p. 1962–76。

55. Borisov N, Danezis G, Mittal P, Tabriz P. Denial of service or denial of security?In:Proceedings of the 14th ACM conference on Computer and communications security。ACM；2007 年。p. 92–102。

56. Sun Y, Edmundson A, Vanbever L, Li O, Rexford J, Chiang M, et al. RAPTOR:Routing Attacks on Privacy in Tor。2015 年 [引自 2019 年 9 月 16 日]；获取位置：https://pdfs.semanticscholar.org/76c7/73bb98b0a266970a589f2cabbd24565b6e19.pdf

57. Johnson A, Wacek C, Jansen R, Sherr M, Syverson P. Users get routed [互联网]。Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security - CCS '13。2013 年。获取地址：http://dx.doi.org/10.1145/2508859.2516651

58. Houmansadr A, Kiyavash N, Borisov N. Multi-flow attack resistant watermarks for network flows [互联网]。2009 IEEE International Conference on Acoustics, Speech and Signal Processing。2009 年。获取地址：http://dx.doi.org/10.1109/icassp.2009.4959879

59. Zhang L, Wang Z, Xu J, Wang Q. Multi-flow Attack Resistant Interval-Based Watermarks for Tracing Multiple Network Flows [互联网]。Computing and Intelligent Systems。2011 年。p. 166–73。获取地址：http://dx.doi.org/10.1007/978-3-642-24010-2_23

60. Yu W, Fu X, Graham S, Xuan D, Zhao W. DSSS-Based Flow Marking Technique for Invisible Traceback [互联网]。2007 IEEE Symposium on Security and Privacy (SP '07)。2007 年。获取地址：http://dx.doi.org/10.1109/sp.2007.14

61. Murdoch SJ, Danezis G. Low-Cost Traffic Analysis of Tor [互联网]。2005 IEEE Symposium on Security and Privacy (S&P'05)。获取地址：http://dx.doi.org/10.1109/sp.2005.12

62. Chakravarty S, Stavrou A, Keromytis AD.Traffic Analysis against Low-Latency Anonymity Networks Using Available Bandwidth Estimation.In:Computer Security – ESORICS 2010. Springer, Berlin, Heidelberg；2010 年。p. 249–67。

63. Panchenko A, Niessen L, Zinnen A, Engel T. Website fingerprinting in onion routing based anonymization networks [互联网]。Proceedings of the 10th annual ACM workshop on Privacy in the electronic society - WPES '11。2011 年。获取地址：http://dx.doi.org/10.1145/2046556.2046570

64. Cai X, Zhang XC, Joshi B, Johnson R. Touching from a distance [互联网]。Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12。2012 年。获取地址：http://dx.doi.org/10.1145/2382196.2382260

65. Rimmer V, Preuveneers D, Juarez M, Van Goethem T, Joosen W. Automated Website Fingerprinting through Deep Learning [互联网]。Proceedings 2018 Network and Distributed System Security Symposium。2018 年。获取地址：http://dx.doi.org/10.14722/ndss.2018.23105

66. Bhat S, Lu D, Kwon A, Devadas S. Var-CNN:A Data-Efficient Website Fingerprinting Attack Based on Deep Learning [互联网]。Vol. 2019, Proceedings on Privacy Enhancing Technologies。2019 年。p. 292–310。获取地址：http://dx.doi.org/10.2478/popets-2019-0070

67. Sirinam P, Imani M, Juarez M, Wright M. Deep Fingerprinting:Undermining Website Fingerprinting Defenses with Deep Learning.In:Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security。ACM；2018 年。p. 1928–43。

68. A Critique of Website Traffic Fingerprinting Attacks | Tor Blog [互联网]。[引自 2019 年 9 月 17 日]。获取地址：https://blog.torproject.org/critique-website-traffic-fingerprinting-attacks

69. Pearce P, Ensafi R, Li F, Feamster N, Paxson V. Augur:Internet-Wide Detection of Connectivity Disruptions [互联网]。2017 IEEE Symposium on Security and Privacy (SP)。2017 年。获取地址：http://dx.doi.org/10.1109/sp.2017.55

70. Humphries M. China Starts Issuing $145 Fines for Using a VPN [互联网]。PCMAG。2019 年 [引自 2019 年 9 月 15 日]。获取地址：https://www.pcmag.com/news/365860/china-starts-issuing-145-fines-for-using-a-vpn

71. VPN Usage Statistics | Global Trends in the VPN Industry [互联网]。GeoSurf。2019 年 [引自 2019 年 9 月 15 日]。获取地址：https://www.geosurf.com/blog/vpn-usage-statistics/

72. Ensafi R, Fifield D, Winter P, Feamster N, Weaver N, Paxson V. Examining How the Great Firewall Discovers Hidden Circumvention Servers [互联网]。Proceedings of the 2015 ACM Conference on Internet Measurement Conference - IMC '15。2015 年。获取地址：http://dx.doi.org/10.1145/2815675.2815690

73. Chen, Chen C, Asoni DE, Perrig A, Barrera D, Danezis G, et al. TARANET:Traffic-Analysis Resistant Anonymity at the Network Layer [互联网]。2018 IEEE European Symposium on Security and Privacy (EuroS&P)。2018 年。获取地址：http://dx.doi.org/10.1109/eurosp.2018.00018

74. Meiklejohn S, Mercer R. Möbius:Trustless Tumbling for Transaction Privacy [互联网]。Vol. 2018, Proceedings on Privacy Enhancing Technologies。2018 年。p. 105–21。获取地址：http://dx.doi.org/10.1515/popets-2018-0015

75. Winter P, Pulls T, Fuss J. ScrambleSuit:A Polymorph Network Protocol to Circumvent Censorship [互联网]。2013 年 [引自 2019 年 9 月 18 日]。获取地址：http://arxiv.org/abs/1305.3199

76. Moghaddam HM.Skypemorph:Protocol Obfuscation for Censorship Resistance。2013 年。54 p.

77. Brubaker C, Houmansadr A, Shmatikov V. CloudTransport:Using Cloud Storage for Censorship-Resistant Networking [互联网]。Privacy Enhancing Technologies。2014 年。p. 1–20。获取地址：http://dx.doi.org/10.1007/978-3-319-08506-7_1

78. Dyer KP, Coull SE, Shrimpton T. Marionette:A Programmable Network Traffic Obfuscation System.In:24th {USENIX} Security Symposium ({USENIX} Security 15)。2015 年。p. 367–82。

79. Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, et al. Generative Adversarial Nets.In:Advances in Neural Information Processing Systems。2014 年。p. 2672–80。