Loki

私密交易、去中心化通讯

作者: Kee Jefferys, Simon Harman, Johnathan Ross, Paul McLean

第 3 版

2018 年 7 月 13 日

Loki 是一种工作证明和服务证明混合的系统，提供了一种独特的方式，旨在为完整节点的运维提供经济激励。Loki 利用该种受激励的节点，在第一层区块链网络的基础上创建第二层隐私路由层。第二层上的最小节点功能被一种名为“Swarm 标记”的新方法监控并实施。Loki 基于门罗币源代码的进阶版，确保所有交易均可实现高度隐私。

本白皮书概述了 Loki 所使用的技术。我们预计：随着 Loki 不断发展，该技术将发生变化。我们将发布白皮书的新版本，体现任何实质性的未来变化及更新。

1 引言

数字通讯与交易中对隐私的需求与日俱增。用户数据正在以前所未有的水平被收集、处理、买卖。从用户浏览数据、电子邮件内容，到信用评分、消费习惯，海量用户数据正在世界巨头公司、大型政府参与者之间收集并销售。Loki 旨在提供一套抵抗审查的工具，让用户在私下进行讯息交易与通讯。

比特币承诺保证隐私，但最终却带来了更高的可追溯性。Chainalysis 和 BlockSeer 等公司利用比特币的透明区块链架构来追踪、跟踪特定的交易 [1]。Loki 建立在门罗币的基础上。门罗币是一种加密货币，被公认为是迄今最安全、最隐私的交易网络之一 [2]。然而，我们也意识到门罗币存在固有的缺点。相对于比特币交易，门罗币拥有比比特币更大的数量级，对带宽、处理器和磁盘空间也有显著的要求。随着网络发展，这会为门罗币节点提供者带来庞大负担，也并未对上述节点提供者对网络做出的贡献提供任何激励或奖励。这导致运行节点成本攀高，经常出现“费力不讨好”的情况。因此，我们引入名为“服务节点”的节点奖励方案，通过为节点提供者提供经济激励来缓解该情况。

若得到适当的激励，服务节点还可提供诸多其他以隐私为中心的功能。重要的是，服务节点网络可让用户匿名发送并接收封包。每个服务节点均作为新型抵抗女巫攻击型混合网络中的中继，从而促进该种私密通讯，同时具备与洋葱路由器（Tor）和隐形网计划（I2P）

类似的特征 [3][4]。此外，该紧急通信网络将被用作去中心化端到端加密消息服务的支柱。该讯息服务名为 Loki 信使，可让用户直接通讯，无需依赖于任何受信任的第三方，不需要要求双方同时在线。

Loki 不仅是私密交易的灵活媒介，而且是去中心化和匿名互联网服务的平台。

2 基本参数

Loki 难度目标（区块间时间）	120 秒
难度调整算法	Zawy LWMA [5]
哈希算法	CryptoNight Heavy
椭圆曲线	Curve25519 [6]

3 CryptoNote 协议的要素

尽管可以在任何加密货币基础上实施全节点激励方案，但 Loki 使用门罗币源代码，因为它为交易提供了高度的隐私保证。门罗币是 CryptoNote 协议的演变，使用环签名、隐身地址和环签名机密交易（RingCT），让用户有能力签署交易并模糊金额，同时保持合理的可拒绝性 [7]。

为了让 Loki 生态系统保持隐私，提供支持内部经济的交换媒介非常重要，而且要在 Loki 独立层之间发生交互时将时间分析的风险最小化。比如，当参与第一层交易服务时，用户永远不应该失去从第二层接收的隐私保证，反之亦然。

3.1 环签名

环签名通过为某项交易构建一系列可能的签名者来运行，其中只有一位签名者是实际的发送者。Loki 利用环签名来模糊交易输出的真实历史。所有 Loki 交易必须使用环签名（不包括区块奖励交易）。极其独特的是，固定环大小为 10 的环签名才能在 Loki 区块链上执行。这意味着：每个输入将从十个可能的输出中的一个中支出，其中包括真实的输出（参见 7.3）。

3.2 隐身地址

Loki 利用隐身地址，以确保接收方的真实公钥永远不会与其交易关联。每次发送 Loki 交易时，一个一次性隐身地址被创建，并将资金发送到该地址。使用迪菲-赫尔曼（Diffie-Hellman）密钥交换，交易的接收者能计算出该隐身地址的私有支出秘钥，从而获得资金，无需透露其真实的公共地址 [8]。隐身地址为交易接收方提供了保护，是 Loki 的一项核心隐私功能。

3.3 环签名机密交易

环签名机密交易（RingCT）最初由门罗币研究实验室提出，作为模糊交易金额的一种途径 [9]。环签名机密交易的当前部署使用的是范围证明。范围证明利用 Pedersen 承诺，证

明发送的交易金额介于 0 到 2^{64} 之间。此范围可确保仅发送非负金额的货币，且不会泄露交易中实际发送的金额。近期，诸多加密货币已提出实施能够大幅减小交易数据大小的防弹加密技术，作为环签名机密交易中传统范围证明的替代方案 [10]。Loki 将利用防弹加密技术，减少节点存储和中继时所需的信息，从而提高可扩展性。

4 服务节点

尽管 Loki 在 CryptoNote 协议上实现了新变化（参见 7），但 Loki 的大部分联网功能、可扩展性均由一组称为“服务节点”的受激励节点来实现。为了建立并维护服务节点，节点提供者的大量 Loki 币在一定时间内被锁定，并为网络提供最低水平的带宽和存储。Loki 服务节点提供者从每个区块获得一部分的区块奖励以回馈其提供的服务。

由此一来，网络为女巫攻击提供了基于市场的抵抗力，解决了现有的混合网络以及隐私为中心的服务存在的一系列问题。这种抵抗力基于供需互动，从而有助于防止单个参与者在 Loki 拥有足够大的权益，进而对 Loki 提供的第二层隐私服务产生重大负面影响。达世币首先推测称：抵抗女巫攻击型网络可能源自于加密经济学 [11]。随着攻击者积累 Loki，循环供应减少，他们反过来施加需求方压力，推动 Loki 价格上涨。随着该种局面继续，购买额外的 Loki 价格越来越高，导致攻击的成本极高。

为了实现该种经济保护机制，Loki 鼓励积极抑制循环供应。尤其是，发行曲线与抵押品要求必须经过设计，以确保足够的循环供应被锁定，并为节点提供者提供合理的回报，以确保对女巫攻击的抵抗性。

4.1 区块奖励

Loki 中的区块奖励分发通过工作证明执行。一个强大、精心研究的系统用于创建区块和交易顺序。矿工收集、将交易写入区块，并收取费用。作为 Loki 中的一条共识规则，每个区块包含多项奖励输出，其中只有一项会奖励给矿工。

挖矿奖励:
除了收取交易费外，45%的区块奖励提供给构建该区块的矿工。

服务节点奖励:
每个区块中的第二个输出（总奖励的 50%）将流向服务节点；或者，若选择了某个中继，流向两个服务节点（参见 6.3）。服务节点根据自上次获得奖励以来的时间（或自注册以来的时间）获取奖励，优先选择等待时间更长的节点。每次在网络进行注册时，服务节点会领到队列中的最后一个位置。若服务节点服务良好、未通过 Swarm 标记从队列中被丢弃（参见 8.3），它会慢慢移动到队列更靠前的位置。队列前面或靠前的节点有资格获得奖励。一旦获得奖励，该节点将再次回到队列中的最后一个位置，然后一步一步靠前。

监管奖励:
区块奖励的最后 5%分配给监管操作（参见 9）; 3.75%发送给 Loki 基金会地址（从每个区块确切得出）；剩余的 1.25%进行保留，用于融资区块的输出（参见 9.2.3）。

4.2 可验证抵押品化

服务节点须向网络证明：它们持有所需的抵押品。Loki 设计中固有的隐私功能让这一点非常困难，特别是无法审计公共地址的余额，或使用查看秘钥来审查向外的交易。

Loki 创新使用时间锁定的输出，从而让 Loki 货币能在一定时间内锁定，直到区块链达到规定的区块高度。在规定的区块高度前，Loki 网络将把支出这些时间锁定输出的尝试无效化。Loki 利用该流程来证明某个特定的服务节点持有某个金额，从而防止抵押品出现混乱。

要注册为服务节点，节点提供者创建所需金额的时间锁定型输出。该输出要在经过至少 21,600 个区块（大约 30 天）后解锁。在交易的额外字段中，服务节点提供者纳入可以接收服务节点奖励的 Loki 地址。该地址还将用作服务节点操作的公钥，诸如 Swarm 投票。钱包可以避免将这些服务节点注册交易被用作混入，因为它们的真实金额、目的地会被泄露，因此无法为交易提供多一层的匿名性。

在每个节点加入到服务节点网络前，根据正在降低的抵押品化要求，其他节点必须单个验证上述节点抵押品开支是否与所需的数量匹配。尽管抵押品交易在 30 天后到期，但钱包将具备选择自动重新抵押的功能。

5 Lokinet

洋葱路由协议可让用户通过分布式网络形成通道或路径，使用多节点作为跳跃，以模糊封包的目的地和来源。Loki 网络上的服务节点将运行低延迟的洋葱路由协议，构成一个完全去中心化的覆盖网络，称为 Lokinet。该网络不依赖于受信任的权威，其状态来自于区块链。用户可以连接到单个服务节点，并创建双向路径，供封包通过。该网络可用于访问称为 SNApps 的内部托管服务（参见 6.2）。用户可利用服务节点出口功能，来浏览外部互联网，而不会暴露其 IP 地址（参见 6.3）。

5.1 低延迟匿名路由协议 (LLARP)

服务节点所有应用程序的基础为匿名路由协议。该协议定义了每个服务节点与对等节点进行通讯的方式。Loki 提出了一种名为低延迟匿名路由协议（LLARP）[12] 的全新路由协议。LLARP 是 Tor 和 I2P 的混合，提供额外的理想属性，超越任何现有的路由协议。此外，LLARP 经过专门构建，以在 Loki 服务节点网络上运行。另外，所有 LLARP 优化均考虑该架构。若想了解 LLARP 的目标，我们最好先对现有的路由协议进行分析，并思考 LLARP 如何对它们进行改善。

洋葱路由器 (Tor)

最近几年，洋葱路由器（Tor）一直是最受欢迎的匿名混合网络。Tor 网络具备高水平的抵抗审查的能力，是一项保护互联网隐私的成熟、宝贵的工具。然而，Tor 并不是一个去中心化的网络，而是一个分层网络。另外，Tor 依赖一系列目录权威。该种权威是由靠近 Tor 基金会的一群志愿者操作的中心化服务器 [13]。这些目录权威旨在执行两个主要功能。第一，他们在网络的节点状态中充当可信任的报告员。当 Tor 用户（或中继）第一次连接到网络时，他们可以连接到十个硬编码的目录权威之一。这些目录权威为用户或中继提供称为“共识”的文件。该种文件提供目前在 Tor 网络上运行（不包括网桥）的所有中继、保护节点和出口节点的列表。此外，目录权威还测量每个中继可提供给网络的带宽。他们进而使用该信息将中继归类，确定节点是否可运行为中继、保护节点或出口节点。

这种高度中心化导致 Tor 非常脆弱。2014 年，Tor 收到可信信息，威胁将攻击目录权威服务器 [14]。若美国、德国或荷兰的目录权威被关闭，那就足以关闭十个目录权威服务器中的五个。这将导致 Tor 网络高度不稳定，新的中继与网络交互能力大幅降低。

由于 Tor 仅允许通过传输控制协议（TCP）进行通讯，Tor 中的通讯方法也将遭到限制。IP over Tor 可能执行，但它缺乏对基于用户数据报协议（UDP）（比如 VoIP）的支持。

隐形网计划 (I2P)

隐形网计划 (I2P) 对混合网络架构采用了不同方法，通过引用分布式哈希表（DHT）维持更高级别的信任敏捷性，从而确定网络状态，而不是依赖于受信任的目录权威 [15]。另外，I2P 还允许传输控制协议（TCP）和用户数据报协议（UDP）流量，支持更大范围的协议交互。但是，I2P 并没有某个稳定的开发流程，并且随着时间推移不断积累了技术债务，特别是在加密使用方面。I2P 使用 2048 位的 ElGamal 加密算法。与椭圆曲线操作相比，ElGamal 加密算法导致加密和解密速度较慢。虽然在 I2P 路线图中存在从 ElGamal 加密算法迁移的计划，但进展较为缓慢。

此外，I2P 缺乏对出口节点的正式支持，意味着网络上的大部分流量在访问内部托管的网站，称为 Eepsites。这极大降低了 I2P 网络接触用户的能力，而该类用户使用匿名网络的主要目的是为了访问更广阔的互联网。

另外，I2P 的构建方式意味着：连接到网络的大多数用户也成为路由器。但是，这也是一个问题，因为最终的网络通常缺乏足够的带宽，无法构建快速路径。混合网中的网速受到每个回路中功能最弱的节点的限制；另外，由于低性能用户在 I2P 中成为中继，从而导致整体性能的降低。

最后，I2P 与 Tor 的不同之处在于：前者提供了交换封包的网络，而不是交换回路的网络。I2P 无需构建所有流量通过的单个更长期隧道，而是建立多条路径，让每个被传送的封包可用于在网络中采用不同的路由。这让 I2P 能透明绕过网络拥塞和节点故障。

I2P 和 Tor 均没有完全缓解女巫攻击。野心勃勃的攻击者具有足够时间和资金来购买大量中继, 进而可以执行破坏用户隐私的时间分析。该种分析的有效性增加了攻击者操作的更多出口节点、中继和保护节点 [16]。Tor 和 I2P 完全由志愿者操作。这些志愿者将自己的时间和资金用于节点操作。我们推测，财务激励（而非利他主义）构建的网络可实现更强的攻击抵御能力，同时提供更可靠的服务。

低延迟匿名路由协议

LLARP 在不需要使用目录权威的情况下运行。相反，LLARP 依赖于通过区块链抵押交易构建的分布式哈希表（DHT），让服务节点充当网络中的路由器。在 DHT 中，带宽不会受到监控或记录。相反，带宽测量和分类由 Swarm（参见 8.3.1）产生。该种 Swarm 评估每个节点并判断节点能否为网络提供适当的带宽。

在开放系统互连模型（简称 OSI 模型）中，LLARP 仅尝试提供匿名的网络层。这意味着：它支持更大范围的互联网协议；此外，如果出口节点从用户数据报协议（UDP）流量 [17] 中通过，它还可将存储文件描述符的开销最小化。LLARP 选择基于封包交换的路由，而不是基于通道的路由，从而实现网络中更好的负载平衡与冗余。

我们不预期（甚至不允许）Lokinet 的终端用户路由封包。这意味着：由于开启服务节点操作所需的大量资本开支，Lokinet 遭受女巫攻击的可能性更小。

6 Loki 服务

与矿工的硬件投资类似，每个服务节点提供者在开始操作服务节点时会冻结 Loki 货币。该种冻结的资本有两个用途。

1. 每个服务节点提供者均对网络的成功有充足的权益。若任何服务节点提供者向网络提供糟糕的性能或出现失信行为，他们会破坏并冒着在网络中贬低自我权益的风险。
2. 这为更激进的强制性提供了机会；若网络能有效限制不诚信的节点获取奖励，那么不诚信的节点必须承担抵押品的奖励损失，以及剩余锁定时间带来的机会成本。

若认为上述观点准确无误，我们可以对表现不佳的节点强制执行惩罚（参见 8.3），然后可以创建服务节点组，进行查询，进而对区块链的状态达成共识，或执行特殊的脱链节点行为（参见 Swarm 8.3）。在 Loki 中，该种行为与联网、存储活动有关。这些脱链活动结合在一起，构成面向用户的应用程序后端。这些应用程序利用这些称为 Loki 服务的理想属性。

6.1 Loki 信使

在 Loki 网络上开发并部署的第一个 Loki 服务将是一个去中心化的端到端加密私密讯息应用程序，名为 Loki 信使。

端到端加密通讯传递应用程序为用户提供了一个发送消息的平台，而不会泄露信息内容。但是，该种应用程序依赖于可能被定位、阻止和关闭的中心化服务器 [18][19]。这些中心化服务模型为通讯方的匿名性带来了高风险，因为它们经常要求用户注册电话号码或其他可识别信息，通过用户的 IP 地址直接连接。该种信息可能通过数据泄漏或合法流程从服务器提取；可能被加以利用，为用户带来不良影响。利用 Loki 网络上的服务节点架构，我们可以提供类似于热门中心化加密讯息应用程序（比如 Signal）的服务，同时具备更高的隐私和防审查性。

6.1.1 信使路由

网络上的消息路由根据接收用户的在线或离线状态变化。当两个用户均在线时，由于消息不需要存储在服务节点上，通信的带宽更高。

在 Loki 中，公钥可作为长期加密密钥，也可作为路由地址。在最简单的情况下，该密钥应该在带外交换，以防止中间人攻击。该种交换应亲自或通过另一种安全交换方式进行（参见用户认证 6.1.2）。

在线讯息

在 Alice 得知 Bob 的公钥后，她假设他现在在线，想创建一条通往他的路径。Alice 查询所有的服务节点的分布式哈希表（DHT），并获得与 Bob 的公钥对应的任何引入集来完成此操作。在 LLARP 中，引入集列出了每个用户所维护的引入器。这些引入器可以建立路径。通过 Bob 的引入器，Alice 现在选择了三个随机服务节点，作为她的出发地和目的地之间的中间跳跃点（Bob 的引入器）。现在，一条路径已得以建立，Alice 和 Bob 可以通过该路径来传输消息。若经过妥当认证，并使用洋葱路由器（OTR）（参见 6.1.2），Alice 和 Bob 现在即可在保持高度隐私的同时进行通讯。

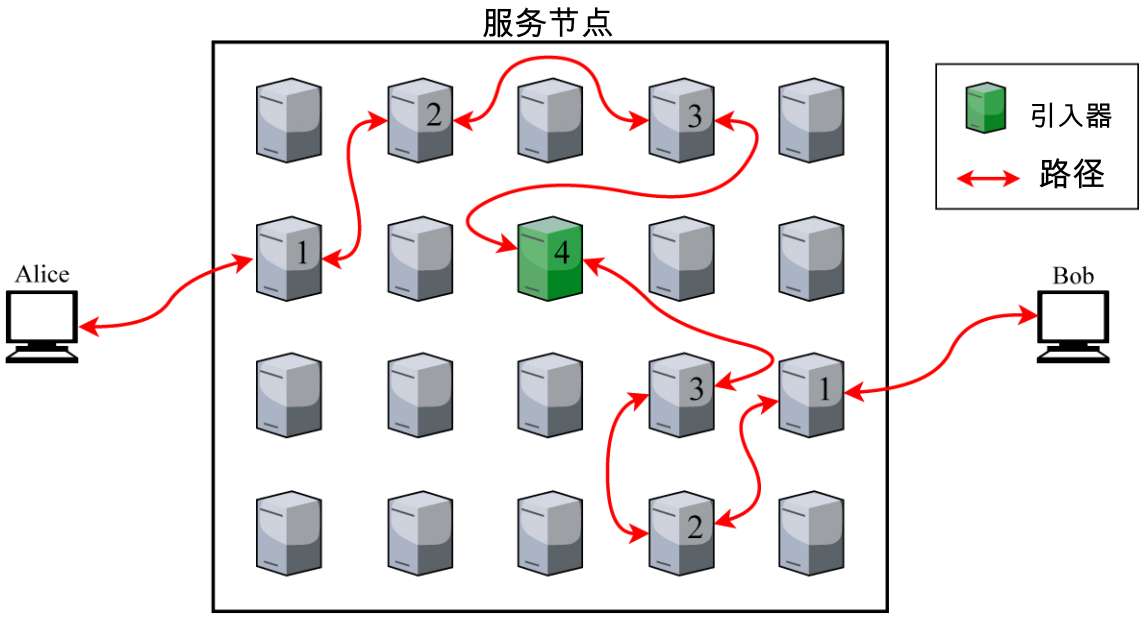

图 1: *Alice* 与 *Bob* 通讯的在线路由的简化版，使用随机服务节点，以建立通过网络的路径。

离线通讯

若 Alice 未能收到 Bob 的回应，她可以启动离线消息通讯流程。离线路由使用 Swarm 消息传递服务（简称 PSS）的进阶版 [20]。Swarm 是服务节点的逻辑分组。该分组基于服务节点的公钥及其抵押交易首次出现的区块哈希。每个 swarm 均有一个由 9 个节点组成的 swarmID。为了向 Bob 发送消息，Alice 可使用他的公钥计算 Bob 所属的 Swarm。借助该信息，Alice 可以匿名将消息通过网络路由到该 Swarm 的随机服务节点中。当收到发往其 swarm 的唯一消息时，服务节点必须将该消息分发给 swarm 中的其他 8 个节点。此外，所有节点必须存储相应分配的生存时间（TTL）中的消息（参见 8.3.1）。当 Bob 上线时，他可以查询自己 Swarm 中的任意两个节点，即可查找自己可以解密的消息。通过附加到每条消息的小型工作证明，离线通讯传递可以免受垃圾信息的干扰（参见 8.2）

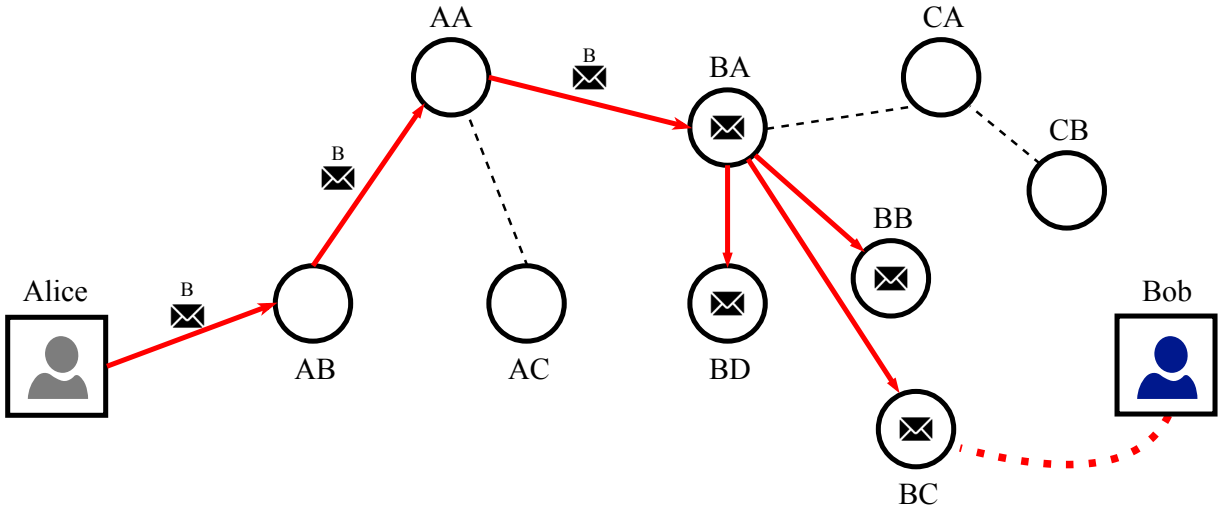

图 2: *Alice* 向 *Bob* 发送消息，分配给 *Bob* 的 *Swarm* 为 *B*；当 *Bob* 上线时，他查询他的 *Swarm* 中的随机节点并接收 *Alice* 的消息

6.1.2 信使加密与验证

一旦建立了消息链，Loki 信使会强制执行向前安全性（简称 PFS）和可否认认证（简称 DA）。PFS 和 DA 是不留记录即时通讯（OTR）协议的关键概念 [21]。很多中心化的服务，比如 Signal 和 WhatsApp，使用保留 OTR 保护的加密功能。Loki 根据现有的 Tox 协议对其 OTR 实现进行建模。Tox 协议是一种去中心化的点对点即时消息协议，使用经过高度审计的 NaCl 库 [22]。

PFS 可以抵御长期密钥暴露的攻击。每个会话均会使用一个新的共享加密密钥。因此，如果单个会话密钥被泄露，整个消息链不会遭到破坏。若第三方企图破解消息链的加密，他们需要获取每个会话的密钥。与现有方法相比，PFS 确保 Loki 信使极难攻破，优于优良保密协议（PGP）加密等现有方法。此外，PGP 只需要一个长期密钥对，即可破坏整个消息链。

可否认认证（DA）指的是双方相互证明自己是每条新消息发送者的能力。然而，第三方无法确定任何消息的真正发送者究竟是谁。使用 DA 时，每次会话后，消息验证代码（MAC）会发布，允许第三方合理创建看起来好像来自发送者公共地址的消息。若实施妥当，任何第三方均无法证明特定消息的发送者到底是不是真实的发送者。

用户验证

用户验证对预防中间人攻击非常重要。比如，如果 Bob 在等待 Alice 的消息，但还不知道她的公钥是什么，那么某个第三方（Eve）可以假冒 Alice 向 Bob 发送消息。这就为什么用户在共享个人信息之前应该相互验证。

与 Pidgin 和其他 OTR 通讯服务一样，Loki 信使使用预分享密钥（PSK）身份验证。用户有多种选择来建立 PSK。他们可以建立一个带外密钥，或者可以通过 Loki 信使询问彼此任何第三方不可能知晓的问题，从而 PSK 达成一致。Loki 将基于 Pidgin 加密认证插件的进阶版来实现 PSK 认证 [23]。

6.2 服务节点应用程序 (SNApps)

SNApps 的功能与 Tor 中日益兴起的隐藏服务类似。它们为用户提供了在混合网络环境中全面交互的一种途径，提供了比访问外部托管内容时更高的匿名性。另外，SNApps 可让用户在自己的机器或服务器上设置和托管市场、论坛、举报网站、社交媒体和大多数其他互联网应用程序，同时保持全面的服务器和用户端匿名。这大幅扩展了网络范围，可以让用户在 Lokinet 内建立有意义的社区。

SNApp 操作者使用传统的服务器-客户端模型，主要区别在于服务节点将成为通过 Lokinet 的用户连接中的中间人。当 SNApp 想在网络上注册时，它必须通过其描述符更新分布式哈希表（DHT）。该描述符包含各种引入器。这些引入器为具体的服务节点专属，供用户互联，形成通往 SNApp 的路径。设置完这些路径后，用户可以连接到 SNApp，同时任何一方均不知道另一方在网络中的位置。

6.3 出口节点

出口节点可让用户向更广泛的互联网发出请求，并通过混合网络返回这些请求。若妥当使用，出口节点可让用户私密地浏览互联网，而不会将用户 IP 地址暴露给服务器。

虽然出口节点操作对 Loki 的扩展实用程式极其重要，但强制所有服务节点全部充当出口节点可能会带来不利影响。充当出口节点可能导致提供者面临法律风险，因为出口节点的

用户可能在将其用作代理时执行恶意活动。由于出口节点仅仅把自互联网的流量中继到最终用户，因此出口节点通常会收到数字千年版权法（DMCA）的请求，或通常被认为是黑客攻击的来源。尽管在大多数司法管辖区，安全港协议可能会保护出口节点提供者，但在其服务器上承载服务节点流量的互联网服务提供商可能会担心法律风险，而且经常会切断对出口节点的服务。

在启动时，服务节点分配到一个中继标志，仅限于在 Lokinet 内的路由封包，但从不向更宽泛的互联网发出请求。若想成为出口节点，操作符必须选择加入，从而表明对额外风险的理解，同时还需提交额外的 Swarm 测试（参见 8.3.1）。

若被选择为区块奖励，选择作为出口节点会为操作符带来比正常的中继奖励高两倍的奖励。提供此激励旨在确保出口节点提供者有足够的财务激励来操作出口节点，有助于预防专门针对出口节点网络的女巫攻击。由于出口节点与中继数比率较低，这是 Tor 自身的一个弱点。

6.4 远程节点

在任何加密货币网络中，存储区块链的完整副本对于众多用户而言不太可能或不太现实。在比特币和以太坊中，用户可以选择连接到保留区块链副本的公共完整节点，可以查询并向网络提交交易。这种模式可以发挥作用，因为比特币和以太坊的完整节点可以有效在区块链中搜索以用户公钥为目标的交易。

由于 CryptoNote 货币的架构，公共完整节点（称为“远程节点”）遭受更大的压力。当用户连接到远程节点时，他们必须临时把每个区块（创建钱包时或从上次检查区块开始）下载到其本地机器上，仔细检查每笔交易，寻找可以从用户查看密钥生成的交易公钥。此流程可能会对远程节点产生显著的性能影响。考虑到该服务无任何奖励，它可能阻止用户为轻量客户运行同步服务。CryptoNote 移动钱包通常不可靠，因为有时必须在建立可靠连接前多次在远程节点间切换，才能扫描区块链或提交交易。

此外，运行少数热门节点之一的恶意远程节点操作者可能在广播具体的交易时记录用户的 IP 地址。虽然该种攻击并没有泄露实际的交易信息，但特定的 IP 地址可与交易相关联，然后可被用来建立与现实身份的链接，从而影响用户的隐私。

通过要求每个服务节点充当一般用户可使用的远程节点，Loki 可以成功规避这些问题。服务节点自然承担该项工作，因为它们已拥有区块链的完整副本，形成了一个广泛分布的高带宽节点网络。通过将服务节点用作远程节点，任何一方持有的远程节点网络均有一个固有的财务限制，从而限制了恶意节点操作者可以收集的数据量。

6.5 Blink

在典型的区块链系统中，任何交易的确认时间是该交易包含在区块中所需的时间。由于矿工相互竞争、隐瞒区块和芬妮（Finney）攻击，接收人通常要求在区块之上创建一些额外区块。在被认定为“完成”前，这些区块一直在保留某项交易 [24]。根据每个区块链特有的海量因素，该流程通常需要 10-60 分钟。对于必须在发送货物或提供服务前等待确认的商家和客户而言，该等待时间造成了不便。

由于 Loki 的服务节点架构，我们可以实现近乎即时的交易。Blink 可让 Loki 主链上发生的相同交易在纳入到区块前得到确认，让发送者和接收者相信交易的有效性，同时保护接收者免于双重支付。

Blink 的工作方式与达世币的 InstantSend 类似。明确选择每个区块、服务节点 Swarm 作为一组证人，确认交易的有效性，锁定交易，以防止双重支付。在该流程中，秘钥镜像被锁定，而不是交易中使用的未支出输出被锁定（比如在达世币中）。秘钥镜像是附加到环签名中每个未支出的输出的唯一秘钥。为了立即提供确认，Blink 授权所选择的 Swarm，向网络发送信号，说明在交易纳入到区块中之前，与该输出相关联的秘钥镜像应被锁定。若发现同一未支出的输出存在双重支付，则产生相同的秘钥镜像，而该镜像将被 Swarm 拒绝，也被整个网络拒绝。

用户将有能力支付更高的费用，来发送 Blink 交易。该交易将在几秒钟内确认，而不需要几分钟。这为 Loki 开辟了一系列新用例，让面对面支付变得越来越实用，在线支付变得更容易整合。Loki 固有的所有隐私功能在整个过程中均不会受到影响。

7 CryptoNote 变更

作为一种加密货币，Loki 在功能上类似于同类 CryptoNote 货币。然而，除了添加服务节点以及相关功能之外，两者还存在一些关键差异。

7.1 ASIC 防御力

专用集成电路（ASIC）是专为单一功能构建的计算机芯片。在挖矿背景下，ASIC 用于计算特定的哈希算法。ASIC 对去中心化造成了一定风险，因为它们超越了所有其他挖矿方法。ASIC 由特定公司制造，硬件的专业性带来非常有限的分销渠道，从而需要大量资本成本来实现有利润的开发和运营。同时，ASIC 具备很多潜在好处，比如挖矿工必须承担资本要求，以投资于特定算法的硬件，使他们不太可能失信操作，从而让自己的投资受损。但是，具有成熟哈希算法的 ASIC 芯片的分布和制造仍集中在少数几家大公司手中。这些公司可能拒绝向某些地区运货，决定哪些地区和客户获得性能最佳的 ASIC，可能构建有限的运行量，以及操纵价格。

为了防止 ASIC 挖矿工垄断网络哈希值，许多加密货币开发了防 ASIC 哈希算法，比如 Scrypt 和 Ethash [25][26]。直到最近，门罗币一直使用 CryptoNight 哈希算法。该算法需要大量的 L3 缓存才可运行。理论上，由于海量的存储器需求，这本应该让生产 ASIC 芯片非常困难。但在 2018 年，Bitmain 发布了 X3。X3 是一种 CryptoNight 专用的 ASIC，可以图形处理单元（GPU）十倍速度有效挖矿 [27]。其他哈希算法遭遇了类似命运。现在，Scrypt、Ethash 和 Equihash 均可被 ASIC 矿机挖矿。

为了对抗 ASIC 的使用，门罗币提出了一种每隔 3-6 个月进行一次硬分叉的策略，以稍微改变 CryptoNight 的哈希算法（第一个分叉转移到 CryptoNightV7 [28]）。构建 ASIC 所需的资金和时间非常重要。另外，凭借高度具体化的硬件设计，哈希算法中的轻微调整会导致芯片设计无效，浪费 ASIC 制造商的时间和资金投入。但是，该方法也存在自身的问题。如果对算法所做的修改不足以阻止 ASIC 被重新编程，网络可能很容易受到哈希值中心化的影响，直到出现另一个硬分叉才可缓解。现场可编程门阵列（FPGA）也应该在防 ASIC 策略中加以考虑，因为对哈希算法不频繁、轻微的改变可能很容易被重新编程为 FPGA。另一个问题是核心共识机制的定期改变会引发可能的意外漏洞，且会围绕核心开发人员团队将该种改变的开发中心化。

业内已提出了许多替代的工作证明算法，应对定期进行硬分叉的需要，包括可证明的内存难解哈希算法，如 Argon2、Balloon 哈希和多态哈希算法（如 ProgPoW 和 RandProg）[29][30][31][32]。Loki 团队将发布关于上述算法的更多研究，以针对 ASIC 抵抗力开发长期的解决方案。

在开展该工作的同时，Loki 将整合一份名为 Cryp-toNight Heavy 的 CryptoNight 版本。该版本保持对 CryptoNight ASIC 矿机的抵抗力。Cryp-toNight Heavy 在诸多方面与 Cryp-toNight V7 有所不同：它将暂存器尺寸增加到 4mb，处理 implode 源码和 explode 源码的方式发生了变化 [33]。这些变化使其与最大的 ASIC 挖矿工目标（即门罗币的 CryptoNight V7）有所不同。此外，在提出更永久的解决方案之前，这些变化带来了更强大的防 ASIC 开发保护。

7.2 动态区块大小

与其他 CryptoNote 货币一样，Loki 没有固定的区块大小。相反，随着时间推移，区块大小会随着网络达到更高的交易吞吐量而增加，以纳入更多的交易。Loki 区块大小通过分析最后 100 区块的中位数大小来拓展，并相应地缓慢重新定位任何新区块的最大尺寸。

其他加密货币存在的一个长期问题是：较大的区块尺寸会给存储和验证交易的节点带来负担。随着区块大小的增加，在更低级硬件上运行的节点无法处理和传播新区块，导致节点网络集中于对维护节点具有商业利益的节点网络中。这可能存在一定的隐患，因为将区块链分布在许多节点上可让链条的状态在诸多不同方之间得到确认，从而增加其有效性和审查抵御性。

在 Loki 中，区块奖励的一部分提供给作为完整节点处理和传播区块的服务节点。由于带宽和性能不足的服务节点从服务节点网络中丢弃（参见 8.3），奖励池会自行执行最低性能要求。该种激励结构可以确保节点数保持在高位。另外，无论区块链规模有多大或带宽要求有多高，该种节点具有足够的性能水平，以在网络上成功分享区块链数据。即使如此，我们依然需要优化交易大小，确保网络有效扩展，以降低服务节点的运营成本，从而可以长期将节点数保持在高位。

7.3 环签名大小

在任何既定的交易中，环签名用于隐藏实际输出。环签名的大小指的是用于构建环的混入物的数量。目前，门罗币的强制最小环签名大小为 7，其中 6 个混入物与交易中真正未支出的输出并行使用。

但是，在论文 0001（由门罗币研究实验室发布）中，对较大环大小的影响研究较少；该论文分析了在区块链上拥有大量输出的攻击者对不同环尺寸的影响 [34]。论文发现：较高的环大小减少了拥有大量未支出输出的恶意攻击者可以执行有效交易分析的时间范围。要求更大的环大小也有助于防止所谓的 EABE/Knacc 的理论攻击 [35]。在该攻击中，第三方（比如交易所）可对两个用户之间的交易执行有限的时间分析。

此外，门罗币并没有网络共识规则强制执行的最大环大小。很多钱包，比如门罗币 GUI，将环尺寸限定为 26 个。然而，用户可以自由、随意手动创建任何环尺寸的交易，只要高于 7。这存在一定的问题，因为大多数钱包的默认环大小为 7。将交易的环大小增加到 7 以上会让它更加显眼（参见图 3）。另外，若某人的交易一直在门罗币中使用非标准环大小（比如 10），被动第三方可能利用时间分析来分析区块链，并推断出模式。

交易哈希	环大小	交易规模(千字节)
3feaff3f48de0bc4c92ec027236165337b64df404aca098e212c1215e9456697	7	13.47
39d484f7c0a2e8f3823a514056d7cb0bf269171cb4582e05955d4c5ee995cad0	7	13.47
e08f5a937e725011bedd44075334ae98dcca32749da231c56da1278d49c0a231	7	13.50
ab35e69d9cca39219c90df8b2b7aab4a54c82127fb1fbaae65d76357f8f76387	7	13.50
6d8ccd56dc2d3eb7de03ba767f0dbf4d5f42ae91e67f4c28f16d6f8b0229c272	10	13.87

图 3: *xmrchain.net*（门罗币区块浏览器）展示了非标准环尺寸为何更加显眼

通过静态强制使用环大小，并将环大小设置为 10，Loki 可以改善这两个问题。静态设置最大环大小有助于保护构造带有 9 个以上混入物的签名环的用户；将环大小最小值设置为 10 可有效防止拥有大量输出的攻击者识别环签名中的真实输出。更大的环大小也非线性地增加了默认的搅拌效应，并随着环大小的增加变得更高效。

在当前交易方案中，将环大小增加到 10 会将交易规模增加 2.6‰。然而，当实施防弹加密技术时，它将占交易规模增加的约 8-13%，因为防弹加密技术会导致交易规模整体下降。由于开销上涨，增加最小环大小可能在网络上带来问题，因为这些网络缺乏支持更大型交易的架构。但对于 Loki，这种负担可以由服务节点承担，因为节点得到激励来操作并提供足够的带宽。

8 攻击预防

8.1 IP 与封包阻拦

虽然服务节点网络没有中心故障点，但网络面临两个重要的审查威胁：验证窃取攻击与深度封包检查 [36][37]。验证窃取攻击目的是收集网络上所有操作服务节点上的 IP 地址，并使用 ISP 级防火墙来阻断与这些特定地址的连接。该审查在中国的 Tor 网络上定期进行 [38]。深度封包检测（DPI）目的是研究通过防火墙的每个单独封包的结构，并选择性丢弃或阻断貌似与特定服务相关的封包。同样，DPI 被大型政府参与者广泛使用 [39]。

业内已做了大量工作，来设计规避 DPI 的系统。用户可利用某些可插式传输，用于改变每个封包的签名，将其显示为正常的未阻断流量。通常，通过运行域前端网桥来避免 IP 阻塞，将流量加密为对 Azure 或 Cloudflare 等未阻断服务的 HTTPS 请求。一旦它们来到未阻断的服务，网桥会将请求转发给所需的位置。在域名前置的情况下，国家级的参与者很难在不大规模中断正常互联网的情况下阻断所有流向热门网桥的流量。

Loki 内置的监管机制（参见 9）可用于操作域名前置网桥，让用户在实施大规模互联网审查政策的国家/地区访问 Loki 的服务。另外，OBFS4 可插式传输支持将与 Loki 钱包发布时的服务节点捆绑在一起，以进一步防止深度封包检测（DPI）[40]。

8.2 拒绝服务攻击

去中心化区块链的用户无需提供数字或物理标识符。这可能对缺乏身份或因身份而受到迫害的用户有益。然而，不需要识别的系统本身易受到女巫攻击，因为恶意行为者会产生大量虚假身份（对于 Loki，大量的公钥-私钥对），并使用这些身份通过请求向网络发送垃圾信息。

众多加密货币一直在尝试解决这个问题，但最终被迫实施按服务收费模型或工作证明模型。在 Siacoin 等按服务收费模型中，用户为自己使用的服务付费。对于 Siacoins，成本由每月每 TB 的存储量决定 [41]。按服务收模型可有效减少女巫攻击，但会导致许多用户远离系统，尤其是类似服务可免费提供时（比如，对于 Siacoin，Google Drive 和 Onedrive 免费服务）。此外，Hashcash 和 Nano 等使用工作证明的模型要求用户在发送消息或交易前计算小型的工作证明 [42][43]。这些小型的工作证明系统比按服务收模式更公平，但却可能成为拥有大量计算能力的攻击者的攻击对象。

Loki 拟议一种经过改良的工作证明方案，以解决 Loki 系统中两个最大的女巫攻击面；离线消息与路径创建。离线消息可能会成为一个潜在目标，因为每条消息必须由 9 个节点组成的 Swarm 存储。若恶意用户超载某个特定 Swarm（带有该 Swarm 必须存储的大量消息），那么可能会出现滥用的行为。在路径创建攻击中，攻击者企图参与尽可能多的节点路径创建流程、占用带宽资源、拒绝对通过网络创建路径的合法用户提供服务。

为了防止这两种攻击，在创建消息和路径时，Loki 网络要求附加简短的工作证明。对于消息而言，该工作证明计算为消息的 Blake2b 哈希值。对于路径创建而言，工作证明与要求将某个节点包含在路径构建过程中的请求一并发送。为确保移动用户的可扩展性、可访问性，工作证明难度要求根据消息或路径的生存时间（TTL）来确定，而不是基于全球网络负载来确定。

8.3 Swarm 标记

当节点在无信任环境中运行、且没有中心化的领导者来强制执行规则时，在网络上维护合适的节点行为会非常困难。虽然 Loki 中的服务节点必须保留正确的抵押品要求，但它们可能选择不在其内存池中路由流量或存储数据。由于该选项有利可图（使用较少的带宽/CPU 周期/存储），我们必须拟定一个分布式标记系统，以丢弃性能不佳的节点。

对于 Loki，该种分布式标记面临着重大的实现上的问题。根本上而言，每个服务节点均由于能得到经济激励，怀有将每个其他服务节点标记为“不良分子”的动机。究其原因，当某个服务节点被标记为“不良分子”时，它将面临从权益池中被删除的风险，从而增加了标记者赢得奖励的机会。分布式标记的一个可行方法是在标记事件发生时提供证据；但该解决方案最终成为制造对其有利的证据的节点的攻击对象。相反，无限制标记让单个节点或成群的协作节点故意标记诚实守信的节点，企图提高他们赢得区块奖励的机会。为了避开这些问题，Loki 提出了 Swarm 标记。

Swarm 标记通过使用现有的 Swarm（参见 6.1.1）来选择将参与每个测试轮的成员。每个服务节点保留区块链的一个副本，由挖矿工创建的每个区块将明确选择多个测试 Swarm。对于每个区块，1%的网络 Swarm 被选来参与测试 Swarm。为计算参与的 Swarm，前五个区块的哈希用于播种梅森旋转演算法（Mersenne Twister）函数，然后按它们在确定性列表中的位置顺序选择 Swarm。

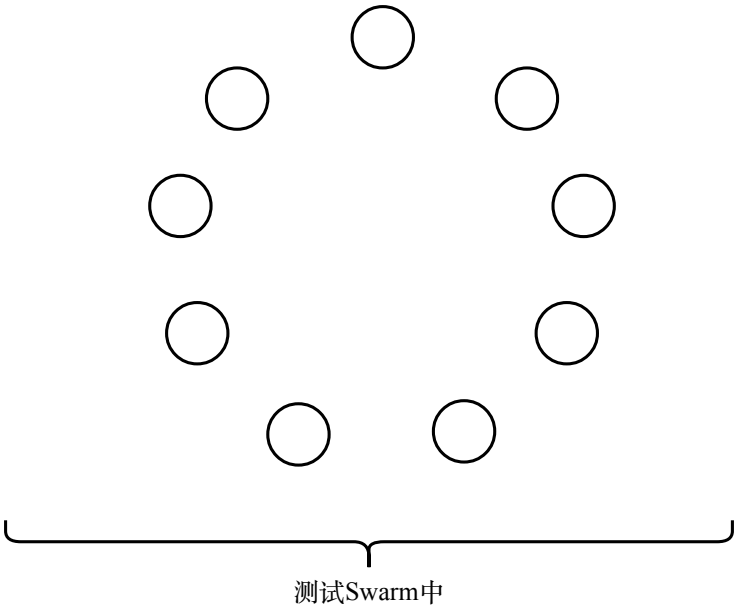

图 4: 测试 *Swarm* 是 *9* 个节点的选定的 *Swarm*

当某个 Swarm 被选中参加测试时，该 Swarm 中的每个节点都会在该 Swarm 中的每个其他节点上进行多次测试。这些并不是主动测试；而是每个节点存储其与 Swarm 中每个其他节点交互的历史信息。随着时间推移，关于带宽、消息存储、区块链请求和出口节点功能的信息将被收集和保留。尚未收集该信息的新 Swarm 进入者可在其所在的 Swarm 外查询服务节点，以在它们测试的每个服务节点上收集数据。

每个服务节点决定了如何对每位 Swarm 成员投票。一旦根据上述测试做出决定，该节点会收集并向 Swarm 广播其投票。现在，Swarm 中的每个节点可检查所有成员的投票。若 Swarm 中的任何单个节点有来自其他节点 50%以上的反对票，任何 Swarm 成员均具有构建注销交易所需的信息。一旦该交易得到验证并包含在区块中，所有服务节点更新其分布式哈希表（DHT）、清除所有经过投票被淘汰的节点。

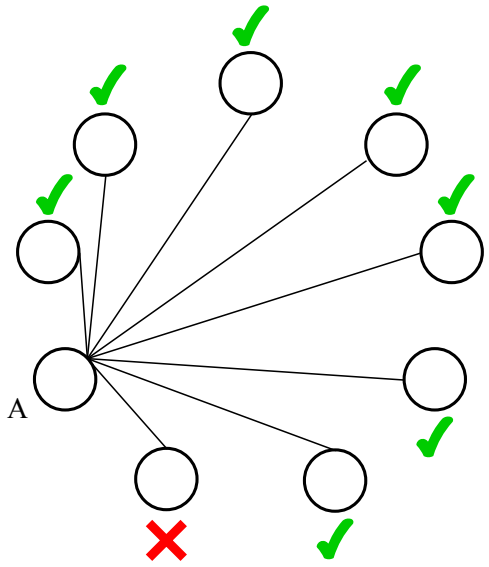

图 5: 不守信的节点由节点 *A* 测试，且未通过测试。节点 *A* 在本地了解哪些节点未通过或通过测试。

8.3.1 测试套件

为了让网络自行执行性能标准，服务节点必须配备所需的工具，以测试其他服务节点。这些测试应涵盖服务节点提供的所有功能，以防止延迟的主节点攻击 [44]。在这个初步设计中，我们提出了四项基本测试。随着服务节点功能的扩展，我们可能在测试套件中添加其他测试。

当节点提供者首次运行服务节点软件时，磁盘上会分配具有预定大小的空文件，以确保需要存储的任务拥有足够空间。然后，在服务节点和由 Loki 基金会运行的一组地理分布的测试服务器间执行简单的带宽测试。这些检查为可选，允许服务节点跳过、忽略或失败，并加入不受信任的服务节点池。但是，运行和传递这些测试为任何可能的服务节点提供者提供了一个良好指示，说明它们是否应冒险锁定可能无法满足最低要求的节点中的抵押品。服务节点加入不受信任的服务节点池后，其抵押品被锁定，并由下一个选定的 Swarm 进行测试。Swarm 测试通过共识执行，服务节点网络的新进入者也无法避开这些测试。若某个节点通过了所有 Swarm 测试，它们将被授予可信任的节点标记，可以开始路由封包。若未能通过测试，它们将从网络中被丢弃，它们的抵押品将被锁定 30 天。

带宽测试

带宽测试构成了 Loki 网络测试套件的支柱。若某个节点通过了该测试，即假设它诚信将封包路由到最小阈值以上。

当每次节点与另一个服务节点交互时，它将生成并保留所提供的进入带宽的记录。随着时间发展，节点将被包含在数千条路径中，路由数百万条消息。这些交互将构成每个节点带宽表的基础。从该带宽表中，节点可响应其 Swarm 内关于服务节点的带宽测试。

我们还预期所有节点响应其他节点的自有带宽表查询。这意味着：最近加入网络的节点也可向更广泛的网络查询有关其 Swarm 中任何特定节点的信息。

消息存储测试

消息存储对 Loki 信使用户的离线消息传递功能极其重要。服务节点须经过测试，以确定其缓存消息的能力，并在消息的生存时间（TTL）内将其提供给用户。

发送离线消息的用户在目标用户 Swarm 中随机选择服务节点。该节点必须在 Swarm 内的其他节点中分发消息的副本。根据附加到消息头部的工作证明，接收副本的服务节点将在生存时间（TTL）内存储数据。当原始消息上的 TTL 结束时，分发节点将该随机的 Nonce 值发送给该 Swarm 的所有其他成员。Swarm 使用该随机 Nonce 值，将其添加到消息中，然后哈希结果，最终将其发送回分布节点。该测试确保服务节点在 TTL 结束前保留消息；如果它们无法生成正确的消息摘要，则会被丢弃。由于分布节点的采样具有随机性，随着时间推移，每个服务节点将可以在其 Swarm 内的其他服务节点上收集性能数据。

区块链存储测试

我们预期服务节点将保留 Loki 区块链的完整副本。通过保留区块链的完整副本，服务节点可执行一系列对网络用户至关重要的任务，其中包括充当远程节点、验证交易以及在 Blink 中锁定交易。

由于诚信的节点也保留区块链的副本，不诚信的节点只需通过在测试时从诚信节点请求区块，即可避免保留完整的副本。为了避免这种不良结果，区块链存储测试经过设计，让保存区块链副本的诚信节点可通过该测试，不诚信的节点则无法通过该测试。

为了实现该目标，测试节点请求每个被测试的节点在区块链的历史内选择 K 个随机交易。然后，这些 K 个随机交易被连接和哈希。接下来，该哈希返回给测试节点。通过测量该请求的延迟，测试节点可将延迟与预期的返回时间 T 进行对比。T 的精确值将得以设置，以准确区分从磁盘加载、从网络下载区块间的预期延迟。对任何攻击者，在 T 时间内下载和哈希 K 个区块应该不可能，因此尾随攻击变得非常困难。

出口节点测试

选择充当出口节点的服务节点可获得额外奖励。因此，我们需要进行功能测试，以确保不会滥用该种额外奖励。

若想执行出口功能测试，服务节点必须能模拟人类的自然搜索行为。若服务节点可以检测到其正在被测试，它只能对测试做出回应，同时忽略合法的用户请求。模拟自然的页面请求行为非常困难。但出口测试可经过设计，让合法请求和测试之间的分类开销变得足够困难，从而让运行合法节点和恶意节点间的带宽成本差异可忽略不计。

服务节点使用一系列本地保留的搜索引擎，辅助以字典，以构建伪随机自然搜索术语。然后，搜索术语被输入搜索引擎，从结果中随机选择网页。现在，服务节点可以构建一条路径，随机节点充当中继，正在被测试的节点作为出口节点。从该出口开始，服务节点请求从其伪随机搜索生成的网页结果。若出口节点返回的结果与服务节点生成的结果匹配，出口节点被认定为通过测试。

9 监管、融资与投票

监管是加密货币设计的重要部分，应在协议级别得到支持。在区块链技术的历史中，业界已广泛研究了脆弱、非正式界定的监管存在的风险。比特币和以太坊经历了有争议的的硬分叉，分散了各自社区的重点和工作。尽管硬分叉可用作监管策略，但它们应始终被视作最后一计，而不是解决每个有争议的问题的常规办法。相比之下，Loki 监管系统旨在通过为话语和代表提供一个结构化环境，从而来解决潜在问题，为 Loki 的发展提供资金，而不依赖于外部影响或利他主义。

除了防止硬分叉外，监管结构应在内部创建途径，以资助可改善 Loki 生态系统的新项目。内部融资项目可防止特殊利益集团的形成，因为这些利益集团不一定具有与用户、矿工或服务节点相一致的动机。我们在比特币和各种比特币分叉中看到了该种盈利公司，如 Blockstream，Bitcoin ABC 以及 Bitcoin Unlimited。业内指责该等公司雇用开发人员对比特币和比特币现金进行针对协议的更改，企图实现自己的业务目标或遵守其特定的意识形态。

由于这个原因，在每个 Loki 区块中，5%的奖励被分配给网络监管。这提供了稳定的 Loki 流，让 Loki 可分布在社区项目、软件开发人员和集成团队中。在这 5%的块奖励中，3.75%由 Loki 基金会控制，1.25%由服务节点通过 Loki 融资系统控制。这种结构鼓励服务节点的公平代表，可实现在 Loki 基金会直接控制外的社区融资提案。

9.1 Loki 基金会

Loki 基金会是一家位于澳大利亚的经注册非营利组织。该中心法律实体旨在让 Loki 项目能在明确的法律框架内运作，为从事项目工作的人员提供法律保护和义务。Loki 基金会在 2018 年于澳大利亚注册成立，实行与澳大利亚慈善机构和非营利机构委员会（ACNC）[45] 相同的宪法。该宪法赋予基金会与诸多其他非营利组织同等的公司监管结构。其中，公司

没有任何股东或受益人，监管会成员各自持有任期限制的席位，通过对其他成员提出的决议进行表决来采取行动。Loki 基金会采用该种结构，以在澳大利亚获得经注册慈善机构的地位。

在宪法上，该组织有义务将任何收入（包括监管区块奖励）用于项目推动和协调。作为一家外部审计的组织，透明度对维持 Loki 基金会的任何经注册慈善机构地位至关重要，并让公众相信 Loki 基金会诚实守信、在合理范围内运营。Loki 基金会对社区及其审计员负责。若该系统最终无法为 Loki 及周边项目服务，我们也提供严谨的保护措施。若出现具有足够网络共识的硬分叉，我们有机会删除或替换 Loki 基金会，避免 Loki 基金会获得该区块奖励。

9.2 Loki 融资系统

虽然 Loki 基金会由代表 Loki 项目的不同 Swarm 组成，但该基金会受制于自己的管理宪法与澳大利亚法律。这可能对基金会的决策范围造成限制。Loki 融资系统可让部分区块奖励纯粹通过服务节点投票来执行。服务节点代表来自世界各地的实体，不受 Loki 项目团队或基金会的限制，让它们在自己的决策中达到新的自主水平。此外，服务节点是网络中最具权益的参与者，因为它们受到经济激励，可以做出增加 Loki 价值的决策。

9.2.1 提案

向服务节点提交的每个提案均发布在 Loki 区块链上。若某一方希望向服务节点提交提案，该方必须构建提案的交易。由于提议的交易内容必须可读、输出必须被销毁，它们放弃了典型 Loki 交易的隐私功能。

每 43,000 个区块（大约 60 天）可创建融资区块。提案负责人可以在此期间随时提交提议。然而，他们也应该考虑到：越早提交提案，他们就有更多的时间从每个服务节点获得投票。

每个交易都附有一个额外字段，包含每个服务节点需要了解的信息，以对提案进行投票。该种信息包括：一个提案标题，链接到提案详尽说明的网址，提案所需要的 Loki 数量，付款地址和托管代理（若选择）。

在征得 Loki 基金会同意后，提出提案的用户也可以选择 Loki 基金会或任何其他第三方作为托管代理人，以在达到里程碑时放款。此外，为了鼓励高标准的提案并防止这些交易发送垃圾信息，每个提案交易必须销毁一小部分的 Loki。

9.2.2 投票

每个服务节点均带有一个特定的投票密钥。该秘钥可导出，也可用于代表服务节点进行投票，而无需登录托管服务节点的服务器。

投票不在链上进行。相反，每个服务节点对区块链上的每个活动提案发出支持、异议或弃权的信号。另外，在下一届每两个月一次的融资区块创建前，服务节点可以在提案被提交区块链之后立即对其投票。在创建下一个融资区块前不久，某个 Swarm 被选定，以收集所有投票数。然后，该投票数被提交到节点内存池，并在某个矿工挖到融资区块前一直停留在内存池中。接下来，该信息用于构建区块，而区块为获胜的提案分配奖励。只有当赞成票数减去反对票数的结果等于服务节点网络上节点数的 15%时，提议才可通过。

9.2.3 资金分配

Loki 融资系统的所有收益均通过融资区块来支付。融资区块奖励的操作方式与传统的区块奖励类似，即以分配 Loki 的完全非监管方式。在每 43,000 个区块（约 60 天）中，一个融资区块由矿工创建。该区块包含整个融资区块在该时期内的整体区块奖励的 1.25‰

为了建立有效的融资区块，矿工必须能评估已达到所需投票比例的提议。这可以使用服务节点提交给区块链的信息来完成，因为区块链包含待付款的地址以及所有投票的状态。所有服务节点将验证矿工的融资区块，并忽略支付无效地址的所有融资区块。

通常，获批提案所需的 Loki 总和将超过或低于上述 60 天内的累计总量。若获批提案的总和超过了融资区块中的可用总额，矿工将优先考虑较早提交给区块链的提案，以此构建融资区块。剩余的获批提案将继续提交给区块链，等待下一个融资区块。

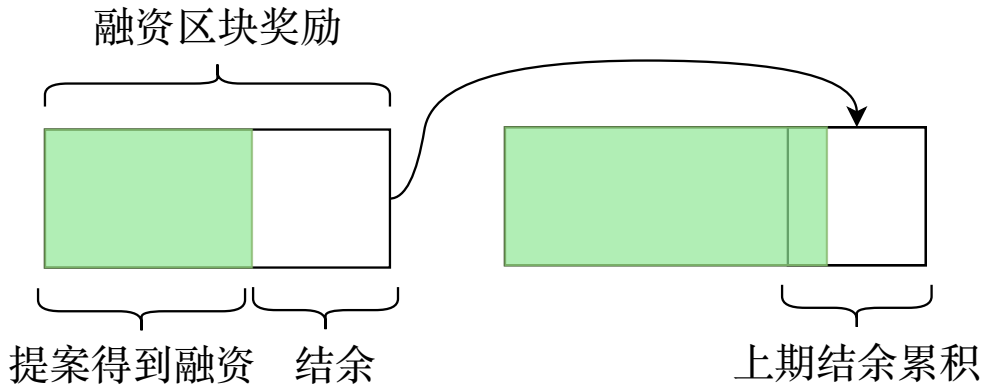

图 6: 未使用的资金作为结余，增加了下一个融资区块的回报

10 结论

Loki 提出了一种基于经济激励型节点网络的匿名交易以及去中心化的讯息模型。Loki 使用 CryptoNote 协议的基础来确保隐私、实施抵押的节点系统，以增强网络韧性和功能。

另外，在先前研究和开源项目的基础上，Loki 提出了进一步改进，展示了一种新的匿名路由协议。该路由协议提供了优于现有协议的显著优势。独特架构和协议设计相结合，实现了基于供需市场、可防御女巫攻击的网络，同时降低了时间分析的效应，并为用户提供了高度的数字隐私。

参考文献

[1] Mike Orcutt, *Criminals Thought Bitcoin Was the Perfect Hiding Place, but They Thought Wrong* (September 11, 2017), https://www.technologyreview.com/s/608763/criminals-thought-bitcoin-was-the-perfect-hiding-place-they-thought-wrong.

[2] *Monero*, https://getmonero.org.

[3] *Tor Project*, https://www.torproject.org.

[4] *I2P Anonymous Network*, https://geti2p.net/en.

[5] *LWMA Difficulty Algorithm*, https://github.com/zawy12/difficulty-algorithms/issues/3.

[6] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters, *Twisted Edwards Curves* (2008), https://eprint.iacr.org/2008/013.pdf.

[7] Nicolas van Saberhagen, *CryptoNote v 2.0* (2013), https://cryptonote.org/whitepaper.pdf.

[8] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Trans. Information Theory **IT-22** (1976), no. 6, 644–654. MR0437208

[9] Shen Noether, Adam Mackenzie, and Monero Core Team, *Ring Confidential Transactions* (2016), https://lab.getmonero.org/pubs/MRL-0005.pdf.

[10] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell, *Bulletproofs: Short Proofs for Confidential Transactions and More* (2017), https://eprint.iacr.org/2017/1066.pdf.

[11] Evan Duffield and Daniel Diaz, *Dash: A Privacy-Centric Crypto-Currency*, https://github.com/dashpay/dash/wiki/Whitepaper.

[12] *GitHub - loki-project/loki-network*, https://github.com/loki-project/loki-network.

[13] *Tor Project: Docs*, https://www.torproject.org/docs/faq#KeyManagement.

[14] *Possible upcoming attempts to disable the Tor network | Tor Blog.* (December 19, 2014), https://blog.torproject.org/possible-upcoming-attempts-disable-tor-network.

[15] Petar Maymounkov and David Mazières, *Kademlia: A Peer-to-peer Information System Based on the XOR Metric*, https://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf.

[16] Philipp Winter, Roya Ensafi, Karsten Loesing, and Nick Feamster, *Identifying and characterizing Sybils in the Tor network* (February 25, 2016), https://arxiv.org/abs/1602.07787.

[17] *OSI model - Wikipedia*, https://en.wikipedia.org/wiki/OSI_model.

[18] Farid Farid, *No Signal: Eqypt blocks the encrypted messaging app as it continues its cyber crackdown* (December 26, 2016), https://techcrunch.com/2016/12/26/1431709.

[19] Matt Burgess, *Russia's Telegram block tests Putin's ability to control the web* (April 24, 2018), http://www.wired.co.uk/article/russia-google-telegram-ban-blocks-ip-address.

[20] *Go Ethereum - Postal Services over Swarm*, https://github.com/ethersphere/go-ethereum/blob/ddfc0a2a02ce574f4c252068ce81f0f5ada1c1ff/swarm/pss/README.md.

[21] Nikita Borisov, Ian Goldberg, and Eric Brewer, *Off-the-record Communication, or, Why Not to Use PGP*, Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society, 2004, pp. 77–84, DOI 10.1145/1029179.1029200.

[22] *NaCl: Networking and Cryptography library*, https://nacl.cr.yp.to.

[23] *Pidgin-Encryption - SourceForge*, http://pidgin-encrypt.sourceforge.net.

[24] *Irreversible Transactions - Bitcoin Wiki* (March 15, 2018), https://en.bitcoin.it/wiki/Irreversible_Transactions.

[25] *Scrypt - Litecoin Wiki - Litecoin.info* (February 12, 2018), https://litecoin.info/index.php/Scrypt.

[26] *Ethash • ethereum/wiki Wiki - GitHub*, https://github.com/ethereum/wiki/wiki/Ethash.

[27] *BITMAIN*, https://shop.bitmain.com/product/detail?pid=00020180314213415366s4au3Xw306A4.

[28] *Monero Cryptonight V7 - GitHub*, https://github.com/monero-project/monero/pull/3253/files/e136bc6b8a480426f7565b721ca2ccf75547af62.

[29] Alex Biryukov, Daniel Dinu, and Dmitry Khovratovich, *Argon2: the memory-hard function for password hashing and other applications* (December 26, 2015), https://password-hashing.net/argon2-specs.pdf.

[30] Dan Boneh, Henry Corrigan-Gibbs, and Stuart Schechter, *Balloon Hashing: A Memory-Hard Function Providing Provable Protection Against Sequential Attacks* (2017), https://eprint.iacr.org/2016/027.pdf.

[31] *GitHub - A Programmatic Proof-of-Work for Ethash*, https://github.com/ifdefelse/ProgPOW.

[32] *GitHub - hyc/randprog: Randomly generate a C (or javascript) program*, https://github.com/hyc/randprog.

[33] *GitHub - curie-kief/cryptonote-heavy-design: Cryptonote Heavy deign essay*, https://github.com/curie-kief/cryptonote-heavy-design.

[34] Surae Noether, Sarang Noether, and Adam Mackenzie, *A Note on Chain Reactions in Traceability in CryptoNote 2.0* (2014), https://lab.getmonero.org/pubs/MRL-0001.pdf.

[35] *Github Comment - EABE/Knacc Attack*, https://github.com/monero-project/monero/issues/1673#issuecomment-312968452.

[36] *I2P's Threat Model - I2P*, https://geti2p.net/en/docs/how/threat-model#harvesting.

[37] *Deep packet inspection - Tec Gov*, http://tec.gov.in/pdf/Studypaper/White%20paper%20on%20DPI.pdf.

[38] Philipp Winter and Stefan Lindskog, *How China Is Blocking Tor* (2012), https://arxiv.org/abs/1204.0447.

[39] *Egypt Quietly Blocks VOIP Services Skype, Whatsapp - TorGuard* (October 26, 2015), https://torguard.net/blog/egypt-quietly-blocks-voip-services-skype-whatsapp.

[40] *GitHub - Yawning/obfs4: The obfourscator (Development mirror)*, https://github.com/Yawning/obfs4.

[41] David Vorick and Luke Champine, *Sia: Simple Decentralized Storage* (2014), https://sia.tech/whitepaper.pdf.

[42] Adam Back, *Hashcash - A Denial of Service Counter-Measure* (2002), http://www.hashcash.org/papers/hashcash.pdf.

[43] Colin LeMahieu, *RaiBlocks: A Feeless Distributed Cryptocurrency Network*, https://raiblocks.net/media/RaiBlocks_Whitepaper__English.pdf.

[44] *Lazy Masternodes: do you actually have to do any work to get paid/vote?*, https://www.reddit.com/r/dashpay/comments/5t6kvc/lazy_masternodes_do_you_actually_have_to_do_any/.

[45] *ACNC template constitution for a charitable company*, https://acnc.gov.au/CMDownload.aspx?ContentKey=2efea0fa-af4f-4231-88af-5cffc11df8b7&ContentItemKey=6046cbc5-d7fd-4b6b-93ba-c8e3114b07ba.