简介：sentinel的愿景

Sentinel生态系统的目的是以一种可信赖和可证明的方式授权普遍接入互联网。这将允许世界各地的组织和个人利用Sentinel基于cosmos的区块链构建具有成本效益的、可伸缩的、分布式和去中心化的网络解决方案。

- 去中心化共识
- 开源网络集成
- 分布式社区节点网络

互联网创造了一种相互交织的全球意识形式，能够产生巨大的积极影响。然而，互联网信息传播能力的重要性和力量正受到威胁。全球互联网审查和海量数据收集的迅速增加，随着当今时代人们对互联网的依赖程度日益提高，这种审查和数据收集的趋势侵犯了获取信息和隐私的基本人权。

Sentinel生态系统最初的重点是为去中心化的建设提供一个框架 虚拟专用网(dvpn)。全球各地的个人都在使用VPN应用程序，他们的目的是通过连接到位于他们想要的内容不受限制的地区的服务器来访问受地理限制的内容，同时通过建立加密连接来确保他们交互的隐私。无论目的是为了访问受限制的内容，还是为了提高他们在互联网上传输数据的安全性，世界各地的个人都要求安全、廉价和可靠VPN服务。

随着允许跨链互操作性的Cosmos IBC的发布，Sentinel将能够在Web 3.0基础设施堆栈中提供一个私有网络或dVPN层。在不久的将来，将有可能构建一个完全分散的DeFi应用程序，即:

- 托管在handshake网络；
- 数据存储在ipfs；
- 利用 Akash network的计算资源；
- 与建立在Sentinel网络上的dvpn集成，为应用程序及其用户提供网络级别的隐私和安全。

在创建之初，VPN技术主要关注于在组织的服务器及其成员之间建立安全隧道，以确保加密的数据传输。在过去的十年里，现代消费者不仅开始将vpn与传统的以企业为中心的叙事联系在一起，而且开始将vpn与一种全新的叙事联系在一起，这种叙事围绕着他们对隐私、互联网安全和全球数据可访问性的关注。正是由于这些担忧，我们见证了VPN行业的蓬勃发展，预计该行业的全球市值将以每年15%的速度增长，在2030达到750亿美元。

目前在VPN领域中，消费者可以使用的VPN应用程序在保证用户“隐私”和“可靠性”的同时，既不能证明其声明的真实性，又不能信守对用户的承诺，这就造成了很大的矛盾。近年来，这种矛盾几乎每季度都被暴露出来，VPN网络一直在故意存储和收集用户数据，与此同时，也存在重大的安全漏洞。VPN行业目前是一个垄断行业，绝大多数领先品牌都共享同一个所有者。与此同时，消费者对这些类似产品的后端功能缺乏信任。

与这些主流的"面向消费者"的VPN应用程序相反，一个强大的、整体的"dVPN"网络(这个术语最初由Sentinel在2017年创造)具有以下优点：

- 可证明的加密：通过开源透明和应用程序完整性验证系统，在用户和用户想要访问数据的服务器之间建立端到端加密的可证明性
- 带宽证明：有一个带宽可证明的系统，允许服务器提供商以一种不可信和可证明的方式提供带宽，以换取用户商定的补偿
- 无日志证明：能够提供证据，证明应用程序开发人员没有集中存储与用户浏览或数据历史相关的日志
- 分布式"出口节点"：拥有一个"出口节点"(dVPN服务器)网络，其所有权分布在许多不知道用户身份的参与者之间
- 分布式中继网络：拥有强大的治理和参与的稳健的中继网络，以降低不良参与者的风险，同时确保退出节点主机不知道用户的身份

参与sentinel网络的利益相关者包括：

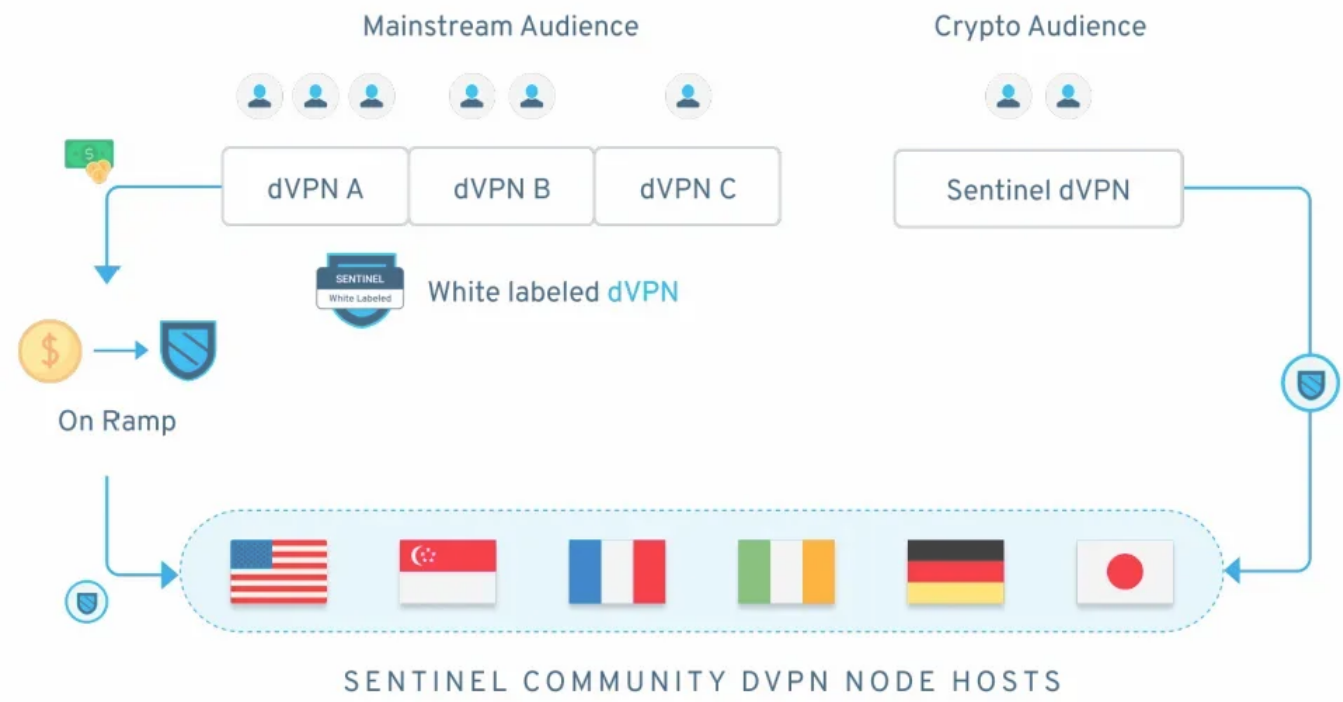
- 验证者：即将到来的Cosmos Hub sentinel的共识参与者，他们负责网络的安全，并参与前哨生态系统的治理
- 用户：终端用户想要访问建立在Sentinel框架上的dVPN，以便安全地访问以一种可证明的方式使用互联网
- dVPN节点主机：社区成员打算通过托管一个出口节点或一个中继节点(满足某些必需的服务水平阈值)，将未使用的带宽提供给建立在Sentinel网络上的dvpn来赚钱
- dVPN应用程序创建者：在Sentinel框架上构建dVPN的创建者，同时使用Sentinel dVPN区域作为其基础设施层。应用程序创建者负责用户获取和营销，以产生收入，以便能够支付dVPN节点主机

去中心化VPN产业

Sentinel不是一个单独的dVPN应用，而是一个独立的网络，dVPN应用程序建立在Sentinel的dVPN协议框架之上。

Sentinel生态系统的目标是使VPN行业去中心化，并将"dVPN"引入主流消费者。然而，这一目标不会通过发布和维护单个面向消费者的应用程序(Sentinel dVPN)来实现，而是通过首先建立和开

发一个框架，可以用来创建一个独立运营的去中心化vpn网络。



建立在Sentinel框架上的dvpn可以由企业实体或个人操作。Sentinel还打算与现有的集中式VPN提供商合作，帮助他们将后端架构过渡到去中心化结构；允许这些公司进一步建立与现有客户基础的信任，同时也允许他们进一步扩展他们的服务产品。

您可能会发现自己想知道为什么企业家或现有组织想要与sentinel合作，建立dVPN?

Sentinel的生态系统缓解了新公司和现有的VPN公司三个进入障碍

- dVPN应用开发的成本和流程：网络协议，如OpenVPN和Wireguard虽然完全开源，但需要打包成可扩展的、安全的"跨平台"应用程序集。同时，集成基于订阅的系统和支付网关提供了开发dVPN网络所需的一些更基本的实现的乏味示例。从头开始开发高端VPN/dVPN应用程序所需的资源需求对大多数人来说都是详细的。

  Sentinel提供开源、跨平台的dVPN客户端，具有弹性、安全性和高度可扩展性。这是因为Sentinel采用了基于cosmos的架构，除了链上节点查询之外，还提供了一个公私钥"账户管理"系统(更多细节将在未来的出版物中公布)。我们确保在Sentinel的框架之上构建和定制架构对开发者是友好的。与自行开发VPN / dVPN应用程序相比，整个过程的成本极具竞争力

- 节点管理和DMCA请求处理：领先的云服务提供商将不可避免地限制服务器访问出口节点主机，因为从该节点流媒体或下载盗版内容无疑会吸引DMCA请求。集中式VPN组织通常必须依赖于"离岸主机服务"，这种服务在运行时间和实时客户支持方面可能无法提供与更成熟的供应商相同程度的可靠性。

  通过整合Sentinel的基于社区的节点主机，Sentinel生态系统消除了在Sentinel框架上构建应用程序的组织的exit-node管理责任。

VPN应用程序的所有者将有能力与Sentinel生态系统中的节点主机创建服务契约并建立一定的质量标准，同时也不必自己管理这些服务器的所有权

- 潜在的安全威胁和与黑客相关的风险：代码闭源和集中式VPN解决方案无法进行同行评审，因此无法由公正的安全专家进行评估。这可能导致潜在的漏洞或安全风险，有能力损害或严重破坏提供服务的公司的声誉。

  安全漏洞的发生不仅将用户置于其数据可能被利用的风险中，而且还会导致VPN组织本身严重缺乏可信度，这可能会极大地影响组织的收入和可持续性。

  Sentinel提供的这种开源结构大大降低了安全漏洞发生的机会。开源软件的优势的一个例子是世界上的军事组织在他们的大多数系统中使用Linux作为他们的首选操作系统。Linux是完全开源的，并且经常受到第三方的审查；而不是像Windows这样的软件套件，它是封闭源代码的，并以安全问题而闻名。

虽然Sentinel框架提供了构建和运营一个强大的dVPN服务的工具和基础设施，但应用程序的所有者有责任获取客户，并了解他们的特定目标市场，以便部署有效的营销策略。需要注意的是，产品开发和执行只是诸多重要因素的一部分。另一部分围绕着用户的实际上手和建立一个市场需要的产品。

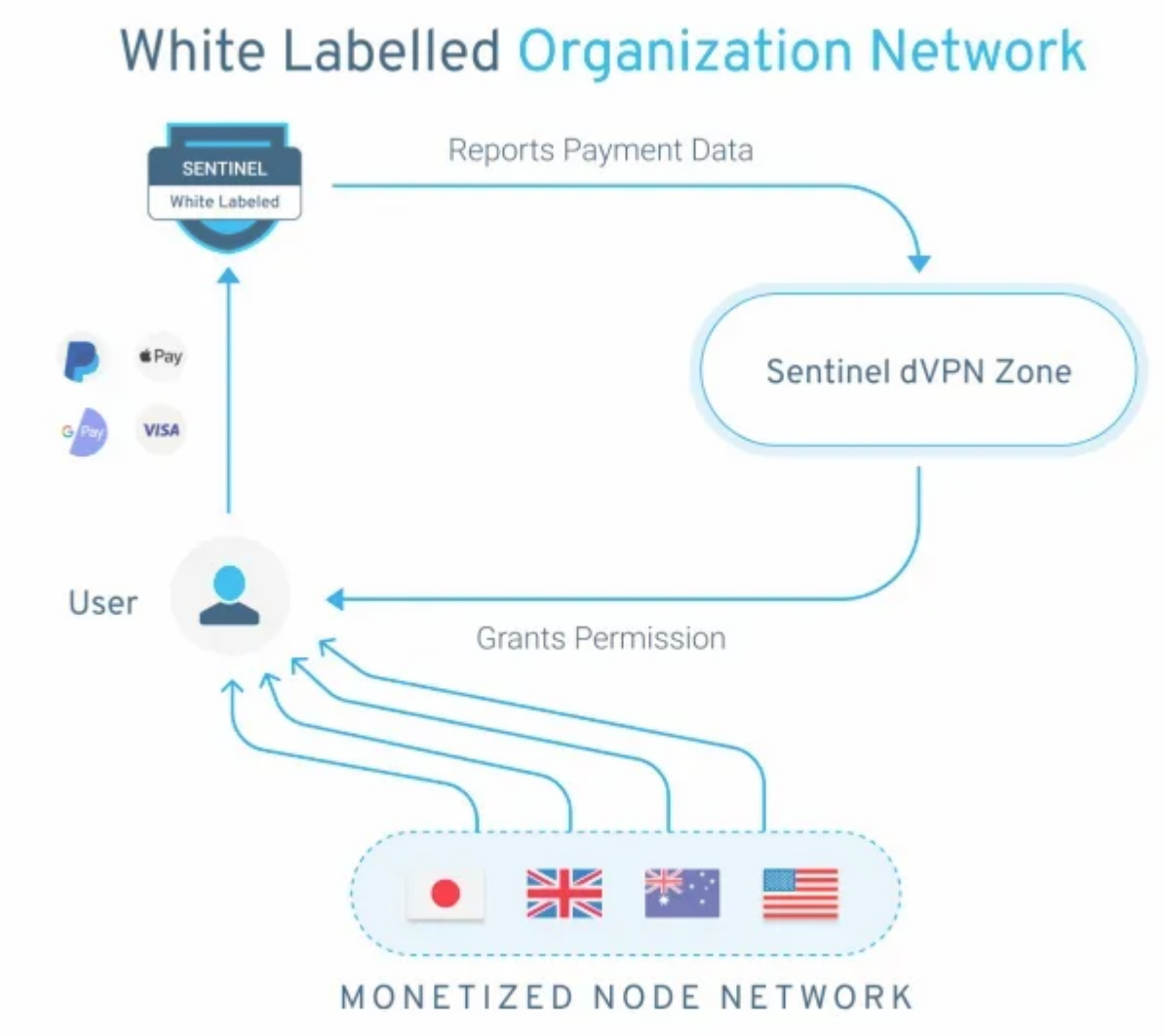
dVPN成功应用的4个关键原则

- 强大的UI / UX：构建在Sentinel框架上的应用程序应该与领先的业界已提供VPN服务的应用程序，就用户友好性和访问方便程度而言没有什么区别。用户可能不愿意过渡到一个更加去中心化的解决方案，除非他们的引导过程是无缝的，即使在需求安全和透明的VPN服务的增长趋势。使用dVPN应用程序的学习曲线必须通过使用智能设计最小化。为了体现一个强大的品牌形象，必须对应用程序的特定美学有很强的关注。

- 有效的定价策略：在尝试建立一个成功的dVPN应用程序时，一个不仅具有成本效益而且有利可图的定价模式的实施起着至关重要的作用。对于应用程序来说，重要的是能够产生收益，然后传递给节点主机。这使他们能够将提供的带宽资源货币化，创造一个健康和可持续的分散经济。所采用的定价模型完全取决于目标人群和应用程序提供的服务类型。未来，Sentinel生态系统中dVPN应用程序的创建者将能够在他们的应用程序中提供高级服务。这些高级服务包括一个区块链框架，用于构建去中心化VPN应用程序即将到来的中继网络，以及其他增强的隐私相关实现。额外的服务可以在用户现有的订阅中定价，也可以根据实际使用的数据量进行货币化。无论dVPN所有者/运营商采用何种定价策略或收入模式，应用程序的开发者都有责任进行适当的尽职调查和分析，以得出最佳定价模式。

- 主流支付网关集成：关键是，基于Sentinel框架的应用程序能够让用户通过基于法币的支付选项进行购买，例如：Visa/Mastercard，Apple Pay，Google Pay，电子钱包（paypal、skrill等）。只有与加密货币相关的支付选项会造成巨大的准入障碍，防止普通消费者轻易地从集中式VPN服务提供商过渡到别处。虽然托管在Sentinel生态系统内的节点必须通过使用基于数字区块链的资产进行支付，但dVPN应用程序所有者有能力通过使用法定支付渠道将其应用

程序货币化。收集到的法定货币可以使用“入站”服务将法定货币转换成数字资产，然后用于支付节点主机。



- 路由协议的多样性：不同的地区需要特定的路由协议来无缝地访问来自互联网的数据，同时避免潜在障碍的干扰。为了在dVPN应用程序中正确部署最佳的“用户特定”路由协议，必须充分理解各种地理位置的复杂性和特性。在一个地理位置无缝执行的网络配置在另一个地理位置可能是完全多余的，因此在为dVPN应用程序选择适当的路由协议时需要定制的方法。例如，OpenVPN协议不能绕过几个不同国家的防火墙，而它在其他国家的功能没有任何障碍。

基于cosmos区块架构sentinel概述

cosmos：去中心化加密货币生态系统的未来

互操作性解决方案促进了各种加密货币的去中心化网络之间的资产和数据交换，能够减少行业中的部落主义。在这种背景下，

“部落主义”指的是去中心化网络在试图建立或显示其相对对手的优越性时所表现出的侵略性倾向。

事实是，某些网络具有独特的服务主张，这是由它们的自定义体系结构和独特的开发重点所支持的。互操作性使生态系统中的参与者能够同时利用这些网络的优点，而无需进行比较，从而实现水平可伸缩性/专门化。

cosmos旨在通过将这些竞争链连接在一起，有效地减少通常会使它们分开的重大分裂影响，从而减少生态系统中的这种"部落主义"。Cosmos IBC模块将允许这些链上应用程序通过迎合更广泛的用户群来扩大其总体目标市场人口，通过使他们能够接受动态跨链支付，帮助轻松获得新客户。

目前，Cosmos和其他高价值和受尊重的网络之间最重要的互操作性举措包括正在建立的从Cosmos到ZCash和Polkadot的互操作性"桥梁"。

Cosmos生态系统使Sentinel能够在"枢纽"层建立和管理自己的原生链。而构建在Sentinel网络上的dVPN应用程序要么位于共享区域，要么位于它们自己的本地区域，这取决于每个应用程序的吞吐量需求。

使用Cosmos构建的链具有维护治理相关自治的能力，同时也确保Cosmos网络中其他枢纽和区域之间的互操作性。

与ERC20代币模型不同，建立在Cosmos上的链将不必在Cosmos的本地代币中支付费用"ATOM"，相反，他们有能力在链的本地令牌中支付。

Hub与Zone结构

Sentinel使用Cosmos Hub/Zone架构，通过在"Sentinel dVPN Zone"（或侧链）上交换所有应用程序特定的交易和数据，同时将与令牌相关的交易和治理抽象到"Sentinel Hub"（或主链0上，来提高dVPN dApp相关的可伸缩性。Zone将通过Cosmos的区块链间通信（IBC）与Sentinel的主链（枢纽）通信。zone可以松散地比作一种"状态通道"，部署它是为了实现高效扩展。

"dVPN"应用程序特定Zone将有自己的共识治理，这很可能是Hub的共识验证器参与者的子集。虽然在Zone层面没有货币价值交换，但验证者的激励和非激励将在哨兵枢纽层面发生。

使用IBC，Sentinel网络的中心与Cosmos Hub和作为Cosmos 网络的一部分的其他中心进行通信。这不仅将使哨兵网络中的服务能够相互通信，并接受本地令牌SENT或其他白名单令牌，而且还可以帮助它们与Cosmos 网络中的其他网络连接。

Sentinel - Tendermint区块链可以托管自己独立运行的dApps和或服务区域通过建立在Tendermint共识之上的特定治理，允许自己的一套验证事务的验证器。

吞吐量

Tendermint使用bPOS共识系统，其中区块链可以设置有限数量的验证器，以实现更快的共识，同时保护网络免受"拜占庭攻击"。

各种P2P通信和隐私解决方案将建立在Sentinel网络上，将依赖于高容量、基于微交易的收入模式。这使得Tendermint区块链完美地支持Sentinel网络，因为它能够实现高TPS（每秒事务数），

特别是与以太坊的"每秒15笔交易"要低得多。

使用工作证明(POW)共识的区块链每秒交易数(TPS)相对用于构建去中心化VPN应用程序的区块链框架速度较慢，而且许多这种共识网络的扩展解决方案需要对专用硬件进行高资本投资。

Cosmos使用了一种独特的bond - Proof-of-Stake共识，在这个共识中，来自固定数量的验证者的投票，具有一定的熵值，在指定的时间点被网络接受。这增加了网络上事务的总吞吐量，因为处理事务的验证器数量有限。

Tendermint的BFT共识系统允许Sentinel网络实现比当前任何现有PoW网络更快的交易速度；PoW网络因缺乏明确的终结性而受到阻碍。在基于bpos的系统（如Tendermint）中，通过使用一个基于轮询的投票系统，利用有限数量的验证器，通过允许令牌持有者将令牌"绑定"到被认为值得信任的验证器，实现了近乎即时的终结。

互操作性

Cosmos的IBC协议的互操作性允许创建一个挂钩（由一个稳定币支持）。这一特性可以开发为不属于Tendermint或Cosmos生态系统的链。

这些zone的效用将主要用于跨链支付。有了这项技术，在Sentinel dVPN网络上运行的社区托管节点可以接受以太坊等加密货币，BTC、PIVX、DASH、NEO、Dfinity、Cardano等以换取带宽。

任何加密货币都可以被集成，无论它是否构建在Cosmos SDK上。这是通过使用"桥接"实现的，这需要在两个网络之间建立一个可互操作的连接。该"Sentinel Hub"将连接到Cosmos IBC，dVPN用户可以使用Cosmos IBC支持的不同货币或稳定币进行支付。

由于IBC协议可以有效地用于具有不同共识机制和结构示图（如ZCash/Cosmos）的不同网络之间的通信，Sentinel认为，通过引入Hub/Zone模型，IBC协议在事务可伸缩性和dAPP相关效率方面非常有效。

由Cosmos网络和Tendermint提供的技术让我们可以设想一个真正的自由市场经济，由"完美的跨链支付整合"来推动，这是迄今为止任何其他平台/网络都不可能实现的。这是创建真正应用于现实世界的区块链应用程序的漫长旅程的第一步。

治理

在Sentinel基于cosmos的主网上，网络治理将掌握在验证者的手中。这些验证器将通过持有者的委托，在基于cosmos的Sentinel主网上民主地确定。验证器的"投票权"（Voting Power）或权重不仅由历史性能决定，还由Sentinel支持者委托给它们的令牌数量决定。

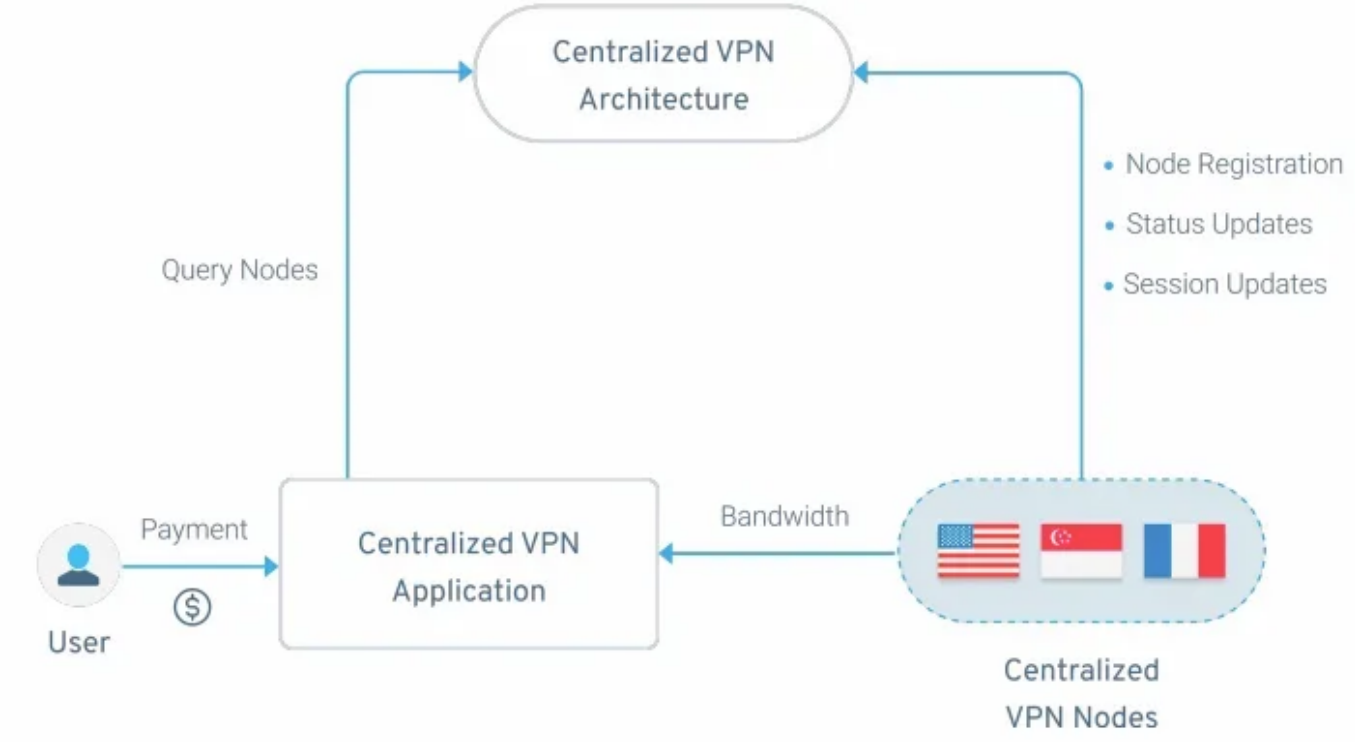
网络治理提案由一组民主的验证者处理，绕过了分叉到"新链"的要求。这些建议可包括：

- 接受新的验证器或拒绝现有的恶意验证器
- 接受新的zone和桥，或拒绝现有的
- 更改供应或锁定一个恶意/黑客帐户

Sentinel dVPN架构概述

集中式VPN架构由多个中间服务器组成，这些服务器用于管理用户的权限，以及建立用户到VPN节点的连接。这种集中式体系结构要求对这些中间服务器有高度的依赖，由于存在多个故障点和多个攻击点，这对网络弹性构成了风险。集中式VPN网络的停机时间可以归因于一个或多个这些组件的功能不正常，并可能导致用户体验和满意度的下降。

与任何消费级VPN相比，Sentinel dVPN框架提供了难以置信的弹性和安全性。Sentinels架构最小化了中间服务器和依赖关系的数量。除了完全在链上进行的帐户管理和创建系统外，查询可用服务器的过程也在链上进行。作为应用程序托管的区块链将24/7运行，没有干扰，全球社区的验证器基础设施是去中心化的（不受1、2或3数据中心故障），这样应用程序的正常运行时间和用户体验将远远超过集中式竞争产品。



Sentinel架构弹性的一个主要贡献因素是计算能力的分散分布，这将需要运行Sentinel Hub和Sentinel Zone。Sentinel dVPN生态系统运行所需的计算能力不是依赖于任何集中式组织提供的，而是由专家"验证"组织提供的，分布在全球各地，具有高冗余系统，具有显著的带宽吞吐量和正常运行时间。

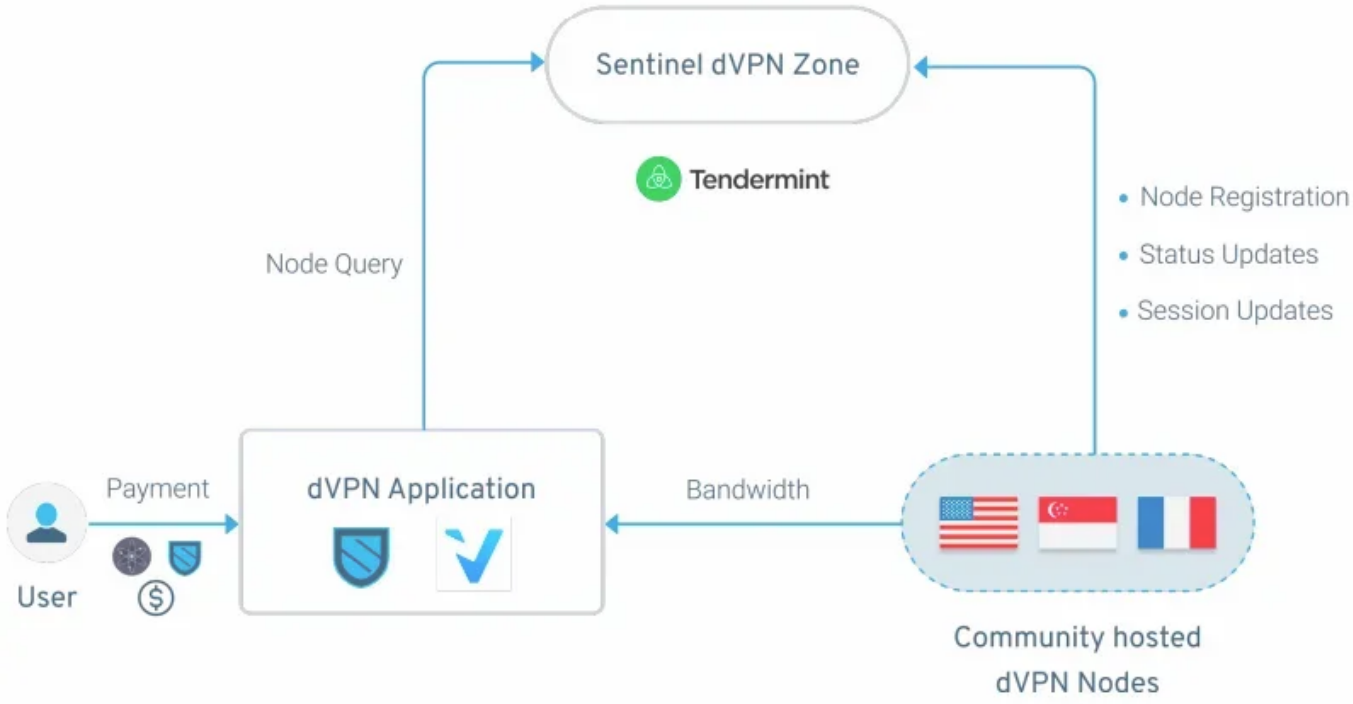
虽然Sentinel的架构确保了用户的匿名性不会受到应用程序本身的影响，但使用Sentinel即将推出的中继网络是必要的，以确保从出口节点的角度来看，用户是完全匿名的。Sentinel 中继网络将允许用户通过一系列的隧道连接"中继节点"，确保用户不直接与出口节点交互。

Sentinel自有的"带宽证明"协议确保了服务提供商（基于社区的节点）向最终用户提供的带宽提供的透明且不可信的度量。"带宽可证明性"协议与Sentinel区块链集成，为所提供的带宽服务的质量提供了清晰的跟踪记录，并在所有参与者之间建立了一定程度的信任。这些数据稍后用于确定节点是否满足所需的服务水平协议，以避免惩罚。

链上查询

Sentinel的"链上"查询系统的实现是Sentinel最重要的技术成就之一，并确保了高度弹性和去中心化的架构。

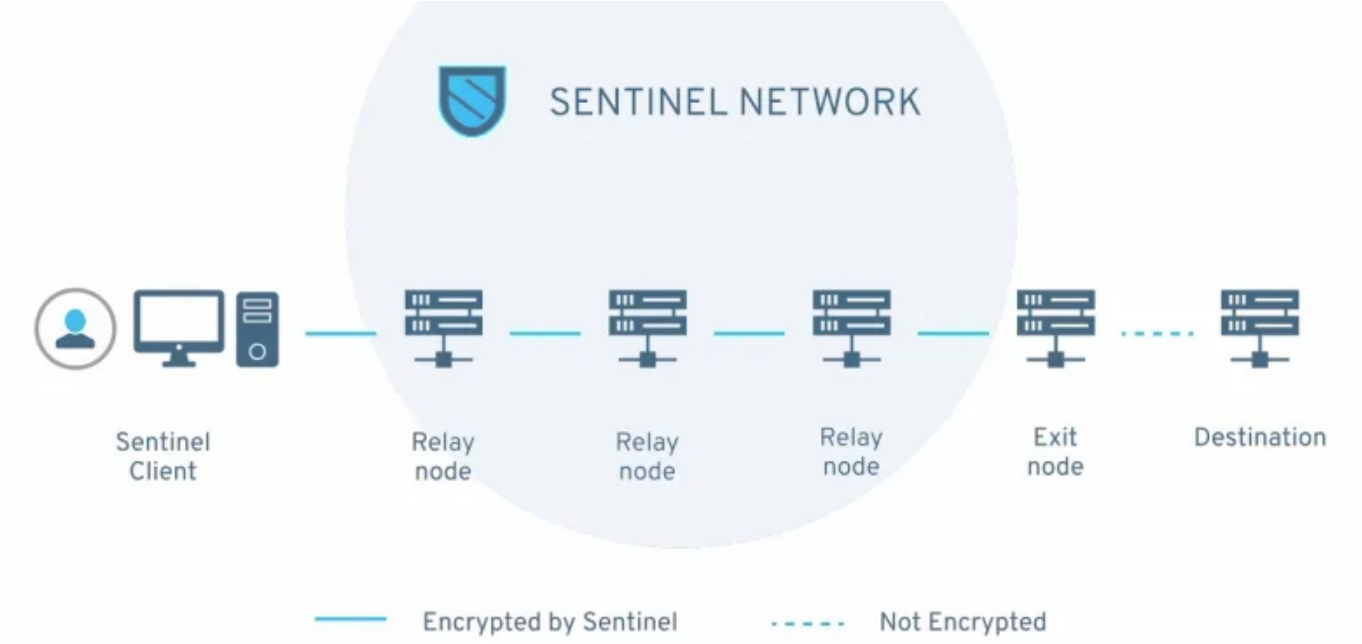
通过Sentinel的dVPN架构，用户和出口节点之间的连接可以直接建立，而不需要连接到由应用开发者或第三方控制的中间服务器（如发现节点的主节点）。这是通过利用区块链作为"节点查询"的分类账来实现的，节点具有与节点属性和连接指令相关的信息进行接口和存储的能力。用户的基于Sentinel的dVPN应用程序将通过从Sentinel专用dVPN区域的事务读取数据，简单地查询所有可用的dVPN节点，填充可用服务器列表。由于认证和身份管理已经发生在链上，理论上Sentinel dVPN dApp结构唯一的故障点（网络女巫攻击除外）成为链级潜在的共识安全故障。危及Sentinel dVPN应用的唯一方法就是危及验证者驱动的共识。



主流的VPN应用程序通常控制出口节点，同时也控制和利用存在于出口节点和用户之间的中间查询服务器，使中继网络的目的冗余，因为原始用户的IP很容易看到。

然而，"链上查询"体系结构意味着用户只需要直接与链通信，而不需要与任何其他可能记录交互的集中式服务器通信。

中继网络



一个强大的中继网络是任何端到端dVPN解决方案的重要方面，它完全维护用户的隐私权。虽然无论是基于Sentinel的dVPN应用程序的创建者还是基于Sentinel的任何参与者，Sentinel区块链可以访问与用户有关的任何个人信息(例如IP地址)，在没有中继网络的情况下，托管在Sentinel生态系统中的一个出口节点可以访问用户的IP地址。而dVPN应用程序有能力提供相关证据，没有日志用户浏览和元数据收集/存储集中到应用程序开发人员，目前不可能证明日志不会被出口节点收集或存储主机本地设备。

为了用更简单的术语来描述中继网络，可以将用户和出口节点之间的连接比作用户向第三方拨打蜂窝电话。如果用户的意图是让第三方无法在来电显示中看到用户的号码，那么用户将不得不使用他们朋友的设备作为中继来屏蔽用户的电话号码。然后，用户必须打电话给让用户等待的朋友，并在合并两个电话之前拨打第三方的号码，从而在不暴露用户数据的情况下连接到第三方。

与蜂窝电话中间呼叫者的例子类似，中继网络由"中继节点"组成。中继节点在操作上与出口节点不同，因为出口节点直接与用户通信(在没有中继网络的情况下)，同时也与internet上的web-server通信。而中继节点只与用户、其他中继节点或出口节点通信。

一个强大的中继网络包括：

- 大量的参与者
- 强大的治理
- 多个网络集成

基于Sentinel的中继系统的使用，将主要针对那些愿意牺牲网速来改善隐私的隐私意识更强的用户。

中继网络的好处只有在大量唯一的参与者开始托管网络上的中继或出口节点时才能实现。如果在任何时候，一个实体控制了网络的很大一部分，那么该实体就有可能通过一个简单但有效的"中间人"(MITM)对用户进行去匿名化。中继网络的主要目标之一是确保中继节点无法识别它们是在向

用户还是另一个中继节点隧道。如果一个用户发生路由流量通过攻击者的中继节点以及出口节点，攻击者能够关联用户的IP地址和反过来确定用户原始请求的信息流并不是简单的另一个继电器的参与者。

在中继网络中拥有一个分布式网络来防止中间人攻击的重要性被比特币生态系统分享，挖矿的目的是防止51%的攻击。如果一个实体控制了比特币网络挖矿哈希率的51%，那么这个实体就有能力破坏网络，通过执行双花攻击网络的完整性。比特币试图通过其激励机制对抗采矿生态系统中的这些垄断风险。这种激励机制根据矿工参与帮助发现和验证网络上新创建的块，为他们提供奖励。如果比特币是一个没有经济设计的志愿网络，它的安全性很可能会受到损害。一个能够访问重要硬件基础设施的强大实体可以很容易地获得采矿网络的多数控制权，一个志愿者驱动网络的例子是TOR网络。在TOR网络中，中继节点和出口节点的参与不受激励。相反，鼓励他们提供服务只是出于对权力下放背后的精神的共同尊重。业内专家担心，TOR网络已经被控制了大量TOR中继和出口节点的实体所破坏。此时，网络上大约有6000个TOR中继节点，平均每天有600万活跃用户。这清楚地显示了基于志愿者的网络的局限性和风险。

Sentinel中继网络的成功完全取决于唯一参与者的数量。吸引这些参与者需要通过网络上的机制进行一定程度的激励。

基于带宽的证明

在真正去中心化的网络中，带宽的分配与工作证明网络(PoW)中的矿工生成哈希值有一个共同的问题。这个问题围绕着服务提供者(或PoW情况下的矿工)滥用或伪造实际工作量的能力。比特币区块链上的矿工的主要职责之一是确认其他矿工的实际工作(或生成的哈希数)，并确保没有人通过钻系统的空子来阻止奖励。同样，在去中心化P2P网络上的带宽分配情况下，也需要一个健壮的体系结构，以防止意图"欺骗"所提供的带宽量的不良行为者。

可以用一个类比来说明对带宽分配网络的可证明性解决方案的需求，即许多移动电话用户向他们的网络运营商提出的关于他们的国际漫游费的令人沮丧的经验。网络运营商提供的大多数漫游计划都对可使用的带宽量有限制，有时甚至按用户使用的总带宽量来计费。经常会听到一些人说，他们完全不信任自己的运营商，因为他们认为自己被多收了钱，也不明白漫游费的带宽消耗是如何计算出来的。

带宽分布的可证明性不仅对以网络为中心的用例非常重要，而且对以存储和计算为中心的用例也非常重要，因为这涉及到大量的带宽利用率。Sentinel生态系统的关键目标之一是开发和实现第一个带宽可证明协议，或"带宽证明"，以允许不可信的带宽共享。用于构建去中心化VPN应用的区块链框架，该协议的范围超出了构建在Sentinel上的去中心化VPN应用，具有与其他分布式p2p资源共享网络甚至主流应用集成的能力。

Sentinel的带宽证明协议的第一个原型实现发生在以太坊链上，由分布式主节点的外部网络支持。这些主节点将观察和测量服务提供商和用户之间的带宽分配，然后将会话的某些属性，如持续时间和消耗的带宽写入以太坊区块链。然后，dVPN应用程序的计费机制将检索该数据，以生成用户必须支付的发票。这个原型架构按照计划运行，但是由于需要一个额外的主节点网络，不能被称为真正的去中心化。

目前正在Sentinel上构建的带宽可证明协议的实现基于Cosmos/ tendermint的网络，涉及从服务提供商和用户两方面生成"带宽签名"。这些带宽签名本质上是由P2P连接在预先配置的一段时间内传输的带宽组成的消息。服务提供者和用户各自生成自己的签名，每个签名都是用各自的私钥签名的，然后这些签名存储在链上以供追溯使用。如果来自用户和服务提供者的带宽交换请求之间出现差异(在预先配置的时间内)，则连接将由于交换中至少存在一个恶意行为者而被终止。

dVPN应用程序开发者确定的带宽签名变量：

- 每个带宽签名产生的时间段
- 用户和服务提供商签名差异的阈值百分比

例子：Sentinel"带宽证明"协议与构建在Sentinel框架上的"XYZ"dVPN集成。签名生成的时间范围为10分钟，差异阈值为10%。在dVPN使用的前10分钟内，服务提供者输入一个表示提供的1.05 GB带宽的链上签名，用户输入一个表示使用的1GB带宽的签名。两个签名之间的差异落在10%的阈值之间，允许已建立的连接继续而不中断。

在下一个会话中，服务提供者的签名代表提供的2 GB，而用户的签名代表使用的1.5 GB，两个签名之间的主要差异超过阈值，导致连接被终止。

支付模式和代管

点对点带宽分配的货币化允许使用比传统VPN行业通常看到的更动态的支付模式。除了一般的"预付费"系统（用户在固定时间内购买订阅服务）之外，带宽提供商（节点主机）也有能力设置他们自己的每单位(GB)带宽消耗的定价。

在Sentinel生态系统上运行的dvpn将可以通过传统的基于法币的选项（如信用卡）以及由Sentinel支持的大量加密货币进行支付cosmos IBC。然而，通过这两种模式的带宽定价将主要以法币计价。

需要注意的是，虽然带宽的支付可以通过加密货币或法币进行，但带宽提供商（节点主机）为托管节点的基础设施支付的费用几乎总是以法币计价的。与基础设施相关的成本包括云计算成本以及电力成本（如果节点主机使用自托管的物理设置）和硬件成本。

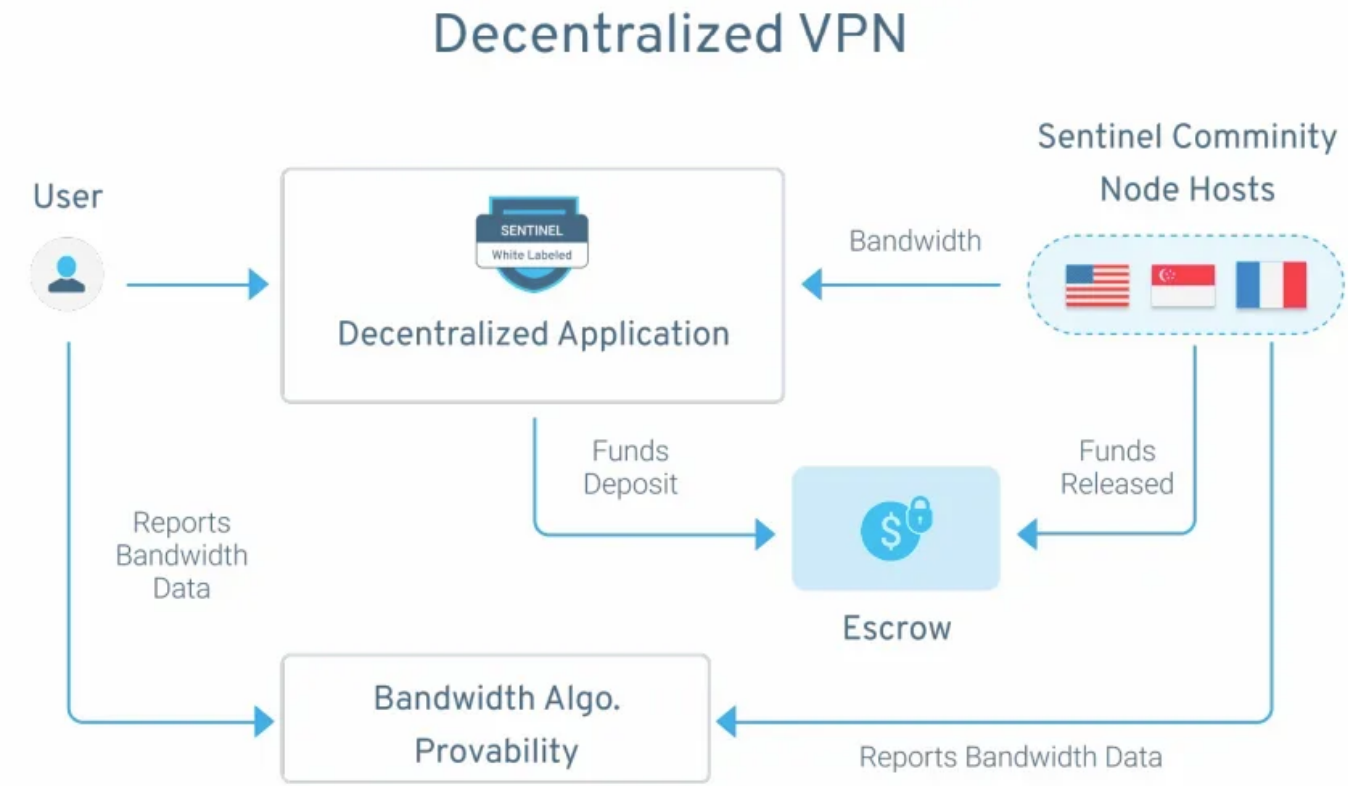
在Sentinel生态系统中，dVPN用户可以使用的两种关键支付模式包括：

- **实时** - Sentinel上的dVPN节点主机使用了一种实时支付模式，允许用户按带宽消耗的单位GB付费。在这种支付模式中，节点主机也有能力为其服务设定自己的价格。
- **预付费** - 预付费模式是一种更传统的支付模式，类似于主流VPN行业中常见的付费模式，即用户购买特定时间段的访问权限。在预付模式中没有带宽消耗的限制，使用通常是无限制的。

Sentinel dVPN托管系统

在用户和服务提供商之间的实时支付模型中使用了托管系统，以确保任何一方都不能以欺诈手段影响交易。在能够建立连接之前，要求用户在托管中锁定一定数量的令牌，令牌将根据用户所消

耗的带宽定期从这个锁定的数量中扣除。提供给用户的带宽的精确测量是通过哨兵"带宽证明"协议进行的，该协议与托管机构通信，以建立一种完全分散的方法来从托管机构释放令牌。



代币功能

Sentinel代币的核心token实用程序围绕其作为：

- 治理和staking
- dVPN订阅的支付方式
- 高级dVPN服务的支付媒介
- 工作token

治理和staking

- Sentinel令牌对于网络安全来说是必不可少的，因为它是Sentinel的Cosmos-based Hub的staking token。Sentinel代币将作为一种"投票权"形式参与治理相关决策，其中用户投票权的大小与他们持有的令牌数量直接相关。
- 用户可以通过将他们的Sentinel代币"委托"给验证器并作为治理的一部分而获得奖励。
- 用户可以托管验证器，并从委托给验证器的代币中赚取佣金。这可以通过请求委托或积累足够的令牌来被认为符合活动验证器集。

Sentinel hub构建在Cosmos SDK上，并遵循与Cosmos hub相同的基于dpos的治理协议和框架。创世纪时验证器的最大数量被设置为50个。Sentinel 中心上的验证器对自委托没有最低要求。

虽然对验证者没有最低的"自我绑定"要求，只有当验证器被委托给自己的验证器的令牌（无论是来自自身还是外部持有者）比授权数量最少的验证器（最后一个验证器，如第50个验证器）更多

时，验证器才有资格进入激活的验证器集。在Cosmos和其他基于Cosmos的网络上，默认情况下也强制执行确定验证器资格的标准。

token持有者有能力通过保护网络来获得奖励。

Hub设定在5%，以确保公平参与和没有立即的最高佣金率。

Sentinel代币的利益相关者也将有能力创建治理提案，或对其他社区成员发布的提案进行投票。这些治理建议提供了编辑链的各种元素或变量的能力，而不需要"硬分叉"，也不需要基于维护的手动关闭链。

dVPN订阅的支付方式

- Sentinel代币可以用于支付dVPN订阅，但这些订阅的支付不限于Sentinel令牌。

dVPN服务的订阅与现实世界中绝大多数流行VPN服务的订阅系统类似。在传统的VPN行业和VPN服务中，很少看到基于带宽计量的计费，提供计量的VPN服务通常提供高级的安全服务和更深层的路由协议。订阅建立在Sentinel dVPN框架上的dVPN服务，需要通过一台或多台设备预先支付无限制使用dVPN的费用。

Sentinel代币将作为订阅支付的一种选择。然而，用户将不仅仅局限于Sentinel代币，因为基于Sentinel框架构建的dVPN应用程序将能够添加现实世界基于法币的支付网关或支持其他类型去中心化货币的支付网关。

通过支付的互操作性，建立在Sentinel上的dvpn将能够通过促进来自主流市场的交易（如谷歌Pay、Apple Pay），获得更广泛的受众。如果订阅的支付仅限于Sentinel代币，客户获取过程将不容易扩大，目标市场将非常有限。

高级dVPN服务的支付媒介

高级服务将要求用户在托管系统中持有代币，该系统将用于实时支付，并由Sentinel的带宽可证明协议管理。这种结构是Sentinel Hub生态系统固有的，因此交易将仅限于本地代币。

建立在Sentinel上的更高级的服务将通过使用托管服务，以及以安全为重点的网络集成，为用户提供增强的隐私和更大程度的不信任。这些服务包括一些应用程序，如中继网络到高度独特和特定于人口的网络协议。高级服务提供商（不是dVPN应用程序所有者）可以提供订阅服务，也可以提供实时带宽计费（按GB付费）的能力。

这些先进的服务将使用Sentinel的"带宽可证明协议"，用于一个分散的治理系统，重点关注实时p2p带宽交换的计量。这种可证明性协议确保没有对带宽提供或消耗的错误描述，而不需要第三方主节点系统来监视连接。

对于这些高级服务的订阅和实时计费，用户将不得不付出自己的代价托管系统中的Sentinel代币。在使用基于订阅的服务时，订阅总持续时间的付款将以分期方式从锁定的令牌金额中扣除。例如：一个高级服务的月订阅可能需要每天从托管的Sentinel代币中扣除总订阅付款的1/30。对

于实时计费，付款将定期从托管中扣除，直接与用户使用的带宽数量相关，提供了一个去信任和安全的事务处理环境。

工作token

- 基于Sentinel cosmos的token作为工作令牌，因此允许代币持有者对代币进行staking以获得奖励。这些奖励是由节点主机生成的，它们为基于Sentinel框架构建的dVPN应用程序提供带宽。

Sentinel的区块链共识的去中心化力量主要依赖于Sentinel Hub的验证者治理中的staking参与。代币持有者将他们的代币staking给可信的验证器以赚取押注奖励，同时通过有效增加恶意攻击的“攻击成本”。作为dVPN服务交换数字资产的交易（加密货币和稳定币）发生在Sentinel Hub，Sentinel代币的持有者将从Sentinel网络上的节点主机产生的收入中获得奖励，作为对生态系统的交易安全做出贡献的交换。

节点主机产生的一定百分比的收益将在池中积累，然后定期支付给token持股人。token持有者从收益分享中获得的价值将与基于Sentinel框架的应用程序对dVPN服务的总需求直接相关。通过建立在Sentinel上的dVPN应用程序产生的用户总数和订阅收入的增加，将导致所需的dVPN节点数量的增加，以满足不断增长的用户带宽需求。

硬件融合

Sentinel dVPN协议与基于Open-WRT（流行的开源路由器固件）的网络路由器集成，将允许路由器所有者通过轻松地利用其带宽赚钱，成为节点主机。此外，Sentinel的目标是支持和集成任何能够在整个wi-fi网络上应用dVPN连接的开源路由器。基于路由器的dVPN将允许用户避免在他们的每一台设备上安装VPN应用程序，用户可能会创建一个仅用于通过dVPN访问的二级家庭网络。

易于货币化

像Sentinel这样专注于“带宽货币化”的生态系统的一个好处是，对于参与者来说，“基于成本”的准入门槛较低，因为在发达经济体中，几乎所有人都拥有稳定和可靠的互联网连接。这种低“成本”门槛的“带宽货币化”可以与挖掘比特币的高“成本”门槛相比较，后者要求用户购买特定的硬件来挖掘和赚取比特币。

Sentinel让世界各地的任何人都可以通过向基于Sentinel的dVPN应用程序提供带宽资源来获得被动收入，而在虚拟机上托管Sentinel dVPN节点需要一定的技术经验。这种“技术”进入障碍降低了Sentinel节点主机社区的潜力，因为它阻止了不太懂技术的用户参与。为了解决操作节点的技术障碍，它不仅需要让普通用户能够非常容易地使用Sentinel dVPN，但必须尽可能简单地托管一个节点，并以提供带宽换取代币。

那些担心在托管出口节点时暴露其住宅IP的用户将有能力托管中继节点。通过托管中继节点，Sentinel支持dVPN的路由器的所有者将能够对互联网服务提供商保持匿名，同时也能够从为这项高级服务付费的用户身上赚钱。

什么是路由器，它们为什么重要

路由器是一种对我们对互联网的依赖至关重要的设备，因为路由器创建了一个网关来连接两个或多个网络。此外，路由器使网络能够方便多个设备，因为路由器确保了负载均衡和带宽吞吐量的分配。

路由器的一般特点：

- 1.建立无线网络的能力
- 2.能够应用加密标准的数据路由通过无线网络
- 3.允许无线网络处理多个设备的能力/负载均衡
- 4.扩大网络覆盖范围
- 5.双波段能力，防止滞后

行业标准路由器有什么问题?

- 1.标准是完全封闭的源代码，不向公众提供进行公正代码审查的能力
- 2.标准路由器不为用户提供通过可验证的dVPN网络建立带宽隧道的能力，dVPN网络提供了安全性和加密的保证
- 3.标准路由器不能为用户提供利用多余未使用的带宽赚钱的能力

这意味着什么

- 1.标准的路由器可以被黑客攻击和操纵，它可能需要几个月甚至更长的时间来发现和修复漏洞，因为代码库是不公开的（例如Linux和微软）
- 2.标准路由器目前还不能为用户提供安全使用去中心化和分布式VPN应用程序的能力，该应用程序能够透明地证明其后端操作的完整性
- 3.标准路由器不允许用户将多余的未使用的带宽货币化，从而导致付费资源的浪费

组织架构

“Sentinel”组织结构主要由“安全网络技术”基金会组成以及专注于dVPN实施和开发的营利性组织Exidio。在撰写本文时，SNT基金会和Exidio都已经完全注册和构建好了。

SNT基金会的重点是将组织和治理方法引入Sentinel分布式生态系统，而Exidio则负责Sentinel dVPN框架的技术开发，以及dVPN应用程序创建者的加入。

“安全网络技术”基金会

- **为定点生态系统项目提供资金和非资金支持** - 负责为存在于Sentinel生态系统中的项目和组织提供非财政和财政支持，这些项目和组织的目标是在Sentinel生态系统上构建并为Sentinel生态系统增加价值。
- **驱动采用** - 通过构思和支持智能用例和实用机制，推动Sentinel代币的采用。
- **确保代币经济可行性** - 任务是确保一个强大的代币经济结构Sentinel的生态系统。有必要监控通货膨胀和其他网络参数，重点是确保代币的价值在长期内不会显著稀释。

- **保证经济健康** - 为生态系统中的验证者/节点/其他服务提供者创建一个健康和富有成效的环境。设计和维持稳健的经济结构，以确保服务提供者能够满足盈亏平衡的成本，并为他们的时间和努力获得合理的报酬。
- **增加生态系统合作伙伴** - 促进Sentinel生态系统和实体之间的合作，为Sentinel生态系统增加价值，并推动协议的使用和token的采用。
- **全球社区的扩张** - 通过维护和支持各区域集团和相应管理区域集团大使，扩大全球Sentinel社区。SNT基金会负责确保生态系统的结构对不同的地区是兼容的，生态系统的设计不会阻碍任何特定的地理位置。

EXIDIO

Sentinel生态系统正在迅速地从一个更隐晦和匿名的网络演变成一个透明的现实世界的生态系统，旨在服务于主流消费者的需求。Exidio是一个专注于实现的营利性组织，通过贡献和实现Sentinel的dVPN和Sentinel的基于宇宙的区块链基础设施，它的使命是"提供Web 3.0的安全访问"。Exidio将与企业家以及现有的VPN公司合作，构建一个新的dVPN应用程序，或者将现有的VPN网络过渡到dVPN网络。

当Sentinel专注于提供一个容纳整体dVPN网络的各种组件的环境时，Exidio将专注于实现白标签dVPN应用程序，并进行必要的定制。

到2027年，VPN行业预计将成为一个超过900亿美元的市场，全球VPN企业家正在利用消费者对VPN服务日益增长的需求，实施白标签解决方案。白色标签的解决方案提供了降低上市成本的好处，并需要更少的技术专业知识和资源来管理。

Exidio对Cosmos的贡献主要围绕以下几个方面：

- **开发工具** - 开发可以由宇宙生态系统中的其他开发人员实现的有意义和创造性的实用程序（例如Exidio multi-sig/联合帐户部署）。
- **开发dApps** - 在Cosmos生态系统中开发有用、高效的去中心化和分布式区块链应用程序（如Sentinel dVPN），能够为主流用户提供真正的实用功能。
- **为Cosmos SDK和Tendermint核心做出贡献** - 为提议的路线图做出贡献，并致力于优化和提高Tendermint和Cosmos SDK当前代码库的效率。

参考

白皮书：https://sentinel.co/whitepaper