PKT网络

Caleb James DeLisle (cjd@cjdns.fr), Jesse Berger (jesse@radicalstudios.com)

2021年2月1日
版本1.0
https://pkt.cash

摘要

互联网是*20*世纪最有影响力的发明之一。然而，在世界上许多地方，互联网接入由垄断行为者控制，他们有权把关互联网的接入，影响公众舆论，限制言论自由。在本文中，我们提出了一个新的网络模型，该模型为将基础设施运营与互联网服务供应商分离开来提供了一个框架。。虽然此模型建立在自治系统和对等关系的成熟概念上，但是还需将这些概念应用到全球网状网络之上的虚拟化域中。为了给这个网络提供资金，我们基于需要大量带宽的工作量证明引入了*PKT*区块链。然后，我们提出了一个去中心化的带宽市场，互联网服务供应商*(ISPs)*从基础设施运营商那里租赁资源，这有助于两个领域的竞争。

1. 引言

互联网从根本上来说是由许多独立的组织组成，这些组织通过共享的物理基础设施租用带宽。通过自愿的联合, 这些组织共同促进了网络中任意两个用户之间原始的、非主观的数据传输[1]。事实证明，该系统非常有效，特别是在竞争激烈、点对点带宽广泛存在的互联网核心区。然而，在世界上许多地方，互联网接入仍然由拥有和运营基础设施的垄断企业控制。为了减少垄断行为，许多国家颁布了本地环路分拆法，要求垄断电信公司与竞争对手共享最后一英里基础设施的接入权[2，3]。虽然本地环路分拆法提高了服务质量, 但也受到了批评[4], 因为这些法律阻碍了基础设施的投资，从而限制了接入。

当互联网接入垄断限制人们可以获取的信息时，公民自由就会受到侵犯。更危险的是大规模监控的影响，它试图对一个定义不清的“敌人”进行全方位的控制，而这个“敌人”可能会扩大到包括社会本身的范围[6，7]。尽管在政治稳定时期，国有化的互联网可以提供高质量、低成本的服务，但它造成了对言论自由和新闻界的权力集中，而在政治动荡时期，这可能会造成灾难性的后果。

我们需要的是一个为人们成为基础设施提供商和服务供应商降低障碍的系统[8，9]。我们提出了一个新的网络模型, 激励人们用最少的技术知识支持互联网接入。这一努力集中分散了互联网基础设施，降低了带宽成本，并激励人们改善全球农村和城市地区的连通性。

1.1. 本文结构

在本白皮书中，我们将介绍PKT网络架构(第2节)。接着我们将描述cjdns以及路由服务器和免费层的集成(第3-5节)。然后，我们将概述PKT区块链的设计，并讨论新型需要大量带宽的工作量证明，该证明激励互联网部署新的基础设施(第6节)。我们对设想中的路由设备硬件（第7节）和去中心化带宽市场（第8节）进行了高层次的技术描述。最后，我们对去中心化带宽市场和促进其出现的技术进行了解释（第9节）。

2. PKT网络架构

PKT网络旨在通过让所有人能够成为互联网服务提供商来分散世界各地的互联网接入。为了虚拟化互联网服务提供商的技术层面，同时分散基础设施运营商在特定地点的作用，我们引入了边缘节点和云互联网服务提供商的概念。边缘节点是由个人、企业或社区团体操控的设备，向公众开放并允许访问PKT网络。云互联网服务提供商是传统互联网服务提供商和虚拟专用网提供商的混合体。云互联网服务提供商集合和代理边缘点宽带租赁，并起到为其客户提供互联网服务的管理作用。PKT网络的云互联网服务提供商系统是围绕两种虚拟资产设计的, 即:虚拟路由器租赁和宽带租赁。虚拟路由器租赁是在一段时间内对路由设备内资源的临时使用权。宽带租用由两个物理路由设备之间的链路上一段时间的最小宽带保证组成。类似于传统的TCP/IP和边界网关协议(BGP)

网络模型[1]，PKT网络促进了云互联网服务提供商之间的提供商、客户和对等关系。这些关系是通过两个关键组件实现的：1)数据包优先级, 2)客户位。

2.1. 数据包优先级

在传统网络中，供应商通常使用较慢的网络链路与客户连接，以控制客户可以发送的带宽数量，从而缓解网络拥塞。然而，这往往导致可用网络资源利用不足。其目的是让PKT网络在网络容量闲置时也允许传送数据包，因此数据包优先权目的是通过现有的基础设施最大限度地传输数据。。

数据包优先级通过数据包头中的优先级字段和一个可配置的称为最大优先级带宽的字段来实现的。通过可配置得最大优先级带宽，云互联网服务提供商能够配置每秒可流经带宽租赁的最大优先级带宽（优先级单位乘以千字节）。如果流经带宽租赁的优先级带宽超过了配置的限制，路由设备就会开始动态降低该流量的优先级，从而保护云互联网服务提供商网络，避免不必要地减少流量。数据包优先级帮助云网络服务提供商选择在链路过载时丢弃哪些数据包。

可配置的最大优先级带宽实际上是特定网络内的带宽份额。如果云网络服务提供商的网络过载，而他们的每个客户都有相同的最大优先级带宽，那么每个客户都将有相同份额的传输数据包。然而，如果一个客户的最大优先级带宽只有其他客户的1/10，那么他们只能通过1/10的流量。随着优先级的成倍降低，每个客户的流量即使从一个云提供商传输到另一个云提供商，其相对优先级也会保持不变。

2.2. 客户位

PKT网络提供对等功能，改进了TCP/IP网络运营商交换流量的方式。传统上，当两个网络运营商签订对等协议时，他们同意直接交换客户的流量，但不为对方承载任何其他流量。这种对等协议是互利的，因此它通常不包括任何类型的财务结算[1]。但是，如果一方发送的流量目的地不是另一方的客户，路由器会将该流量转发给其上游供应商。使用付费连接将这种类型的流量发送给对等方，相当于偷窃。TCP/IP互联网中的网络运营商会根据具体情况处理这些对等的不正当行为，因为他们没有技术可以直接防止这种行为。PKT网络通过在数据包报头中包含一位“客户”字段以及两个可配置项来改进此功能：1)清除客户位, 2)取消非客户优先级。

带宽租赁中任何带有清除客户位可配置集的传入流量都会被清除客户位。这表示有关带宽租约将网络连接到对等方或提供商。非用户可配置的去优先级会影响带宽租赁的输出流量，因此，如果客户位未设置，那么数据包的优先级将降低到不超过指定值。由同一个云网络服务提供商控制的两台虚拟路由器之间的带宽租赁不会设置这两个可配置项。

3. CJDNS

为了理解PKT网络的体系结构，首先我们要介绍一种叫做cjdns的开源网络技术。

Cjdns是一种开源网状路由协议，旨在创建易于配置的分散式网状网络，但在面对敌对参与者时具有强大的安全特性。Cjdns使用始终在线的端到端加密和加密生成的IPv6地址。由于每个IPv6地址实际上是一个密钥指纹，因此所有cjdns流量都可以进行加密和认证，而无需PKI或其他类似的中央机构。IPv6地址位于fc00::/8唯一的本地地址空间[10]中，该空间足够大，因此地址冲突的风险可以忽略不计。

Cjdns部署了一种称为紧凑源型路由的技术。cjdns不是每个数据包都包含其目的地的IP地址，而是包含到达目的地的路由。此外，cjdns用一个紧凑的表示方式来表示这个路由，大小和IP地址差不多。通过将“您想去哪里”替换为“您想如何到达那里”，cjdns优化了数据到达目的地的最佳方式。Cjdns自2011年开始开发，目前活跃在Hyperboria网络中[11]。

4. 路由服务器

为支持路由器的高效虚拟化，路由过程中的决策由属于每个终端用户的云互联网服务提供商的路由服务器来协调。路由服务器使用cjdns紧凑型源路由通过PKT网络提供预先计算的路径。由于数据包转发决策是在cjdns中预

先确定的, 因此路由设备不需要保持任何重要的状态来执行。为了让客户端设备通过PKT网络学习路径，对源路由的解析进行查询，类似于DNS查询。该查询是针对路由服务器进行的。

在PKT网络模型中，网络中的每个设备都与某个路由服务器交互。路由服务器以软件形式实现，因此解析路由的新技术可以随着时间的推移得到改进。如果设备没有已知的路由服务器，它会询问最近的邻居，类似于使用DHCP来查找DNS服务器。除了根据需要进行路由查询之外，网络中的设备还会定期发送有签名、有时间戳的消息, 这些消息包含所有直接连接到它们的设备的身份(密钥指纹)，以及链路质量和宽带租用的相关信息。由于这些消息都是经过签名的，因此任何拥有这些消息的路由服务器都可以立即对其进行验证。cjdns紧凑型源路由与路由服务器的结合将允许云互联网服务提供商使用软件定义的网络(*SDN*), 使其在控制网络方面具有极大的灵活性。我们预计云互联网服务提供商将从虚拟专用网络(*VPN*)服务提供商发展而来，他们也可以通过本地边缘节点提供互联网接入方式。

5. 免费层

PKT网络使云互联网服务提供商能够使用宽带租赁和虚拟路由器租赁来构建网络，因此除非物理链路饱和，否则不会丢弃任何数据包。此外，我们建议每个物理链路都应该有一个可用的免费租赁，这是一个硬接线的无主带宽租赁，保证宽带为零。此外，每个路由设备都应该有一个无主的虚拟路由器，该路由器始终与每个物理链路上的自由租赁互连。这样就形成了一个免费层，在基础设施闲置的情况下，它允许免费使用带宽。
我们认为，浪费资源，同时因为人们无力支付而不让他们使用是不道德和低效的。免费层支持两项关键服务：1)它允许云互联网服务提供商在购买带宽租赁之前执行带宽、延迟和抖动测试，2)它可以防止意外的错误配置。如果某个路由设备配置错误，并且其租赁持有人无法访问，则可以接入免费层以访问该设备的机载计算机。本质上, 免费层的存在改变了多种故障类型的失效模式，从出故障时自动关闭变为出故障时自动打开。

6. PKT区块链

PKT网络利用区块链[12]高效激励节点成为边缘节点和云互联网服务提供商。基于比特币的代码库，PKT用PacketCrypt取代了比特币的SHA-256哈希算法，这是有史以来第一个需要大量带宽的工作量证明。PKT还引入了一种名为“网络管家”的新型机制来资助开发，包括互联网基础设施和网络技术。

6.1. PKT币

节点通过消耗带宽、CPU时间和执行加密来支持网络, 以铸造新的PKT代币投入流通, 称为*PKT*币。PKT 币激励矿工以提高边缘地带的网络吞吐量。PKT币旨在实现微交易的可扩展性，1分钟的区块时间使其比比特币快10倍, 每枚代币的原子单位略高于10亿，而不是比特币的1亿。在63年的时间里，总共将发行60亿枚代币，所有代币都没有中央发行机构。区块奖励会进行循环衰减，即每100天分配减少10%。每次递减都能保证发行量的平稳衰减。

6.2. PacketCrypt

PacketCrypt工作量证明允许矿工之间的通信代替处理器工作，使得最优的挖矿策略对带宽的要求很高[13]。挖矿分为两个不同的阶段：公告挖矿和区块挖矿。在公告挖矿中，CPU工作被消耗，导致创建许多1KB的公告这些公告的结构无法被有效压缩。在区块挖矿中，挖矿者预先提交他们所收集的公告的默克尔m树根，然后对所收集的公告集执行内存依赖挖矿算法。区块挖矿算法每个哈希周期访问4个随机公告，当区块挖矿者发现一个成功的结果时，他们提供所访问的公告以及将它们链接到其预先提交的默克尔分支，从而从统计上证明他们拥有他们声称已经得到的公告数量。这使区块矿工不可能假装拥有他们实际上没有的公告。公告的价值会不断衰减，直到变得无法使用, 所以区块矿工受到激励向公告矿工支付报酬, 以获得稳定的新鲜公告供应[公告挖矿被设计成在CPU上最有效。区块矿工可以挖掘他们自己的公告，但他们将不得不与临时公告矿工的闲置计算资源竞争]。公告挖矿算法使用随机程序来支持CPU而不是GPU或ASIC挖矿，这鼓励在其他闲置资源上挖矿，而不是在集中式农场中挖矿。区块挖矿算法仅依赖于内存硬度，使得GPU硬件成为区块挖矿的良好目标。这两种算法都使用加密操作, 因此高性能挖矿设备也将对VPN数据包加密有用。

任何由工作量证明发行的加密货币都必然会对相关工作产生人为的市场需求。在一个纯粹静态的经济分析中，工作量证明浪费了原本可以很好利用的资源。然而，在实体经济中，我们看到需求推动供应，最终导致成本下降。PacketCrypt旨在创造对带宽的后台需求，我们预计未来将推动加大对网络基础设施投资，并降低带宽成本的进程。

大量带宽挖矿和矿工协作的结果促进了网络效应，包括分散、低延迟网络连接和加密的扩展。这种网络效应对于cjdns以及支持商品市场(包括分散式带宽市场)非常有用(第8节)。

6.3. 网络管家

PKT在区块链的设计中执行了一个网络管家，这个地址从每个新的区块获得20%的PKT币。网络管家的存在是为了PKT生态系统的发展提供资金。网络管家可以通过基于权益证明的投票方式进行更改。投票是通过对交易输出的附加元数据进行 “标记 ”来进行的。活动投票是那些包含此类元数据的未使用事务，因此花费事务输出会撤回投票。每个投票元数据可以包含两个PKT地址，一票赞成，一票反对。当反对现任网络管家的票数之和达到迄今为止所有PKT币的50%以上时，共识规则将确定支持票数最多的PKT地址，该地址将成为新的网络管家。

网络管家是一个为PKT生态系统的发展提供资金的系统，在此系统中，项目提案不得给与任何一个参与者(包括申请人)不公平的利益。这种竞争性的研究模式会不时产生项目预算需求，并根据网络管家的标准对项目提案进行相互评估。网络管家政策鼓励所有被接受的项目围绕开发开源软件、公共文档进行结构设计，并鼓励增加PKT网络的基础设施。所有正在进行的资助项目、已完成的和被拒绝的提案都可以在网络管家的git库中公开找到[12]。如果网络管家没有在PKT币铸造之日起90天内动用其钱包地址中持有的资金，那么这些币将被烧毁[截至2021年1月23日，PKT276,889,678.84已经被烧毁]。通过这种方式，必须对每个项目提案进行评估，以使任何给定的项目提案必须产生的价值对PKT网络的益处要远大于烧毁PKT币。

7. 路由设备

PKT网络的可扩展性要求开发一种高性能的可细分路由设备。这项硬件创新将指导和支持PKT网络的可扩展性。为了确定优化的PKT网络硬件实施的基本要求，我们必须了解在硅中执行这种设备的复杂性，并探索数据包在设备中的流动情况。

数据包通过其物理网络链路进入路由设备。传入的数据包被标记，表明它属于哪个带宽租赁以及数据包优先级。数据包遇到的第一个处理过程是根据最大优先级带宽重新确定优先级。这需要带宽/优先级测量仪，如IIR滤波器。

设备将解析紧凑型源路由标签，以确定数据包应该发送到哪个带宽租赁。然后，设备使用cjdns切换算法更新紧凑型源路由标签，以显示数据包的来源[11]。Cjdns需要访问一个小的索引表，以便计算物理接口号并确定用于发送的带宽租赁标记。

一旦路由路径被解析，数据包将进入一个交换电路。crossbar和clos等架构已经上市[14,15,16]。在数据包离开设备之前，将决定是否需要丢弃数据包。这应该使用具有两级层次的令牌桶架构来实现，其中一级层次是基于传出带宽租赁的保证带宽，二级层次是基于公告的数据包优先级。这是简单以太网交换机中常用的技术。

8. 去中心化式带宽市场

当路由设备连接到PKT网络时，它将立即1)开始测量和公布每个网络连接上的可用带宽和其他指标，2)创建一个令牌来代表每个网络连接上的带宽以及其虚拟路由器，3)开始在去中心化带宽市场上出售这些令牌。这些令牌可以由不同的参与者买卖，并且任何拥有这些令牌的人都可以通过向路由设备发送签名的配置请求来使用底层宽带和虚拟路由器。为了实现这一目标，我们需要建立一个令牌发行成本接近于零且几乎无交易摩擦的去中心化带宽市场。使用HTLC原子交换技术已经可以实现近乎无摩擦的资产交换[17]，这一技术目前正由OpenDEX项目开发[18]。为了使令牌发行成本接近于零，我们正在研究多种不同的解决方案。

8.1. TokenStrike

令牌化带宽和路由器资源有一个有趣的特性，那就是“只和它们的发布者一样好”，因为在最坏的情况下，发布者可以简单地关闭路由设备。这个属性意味着，只要发行者不能秘密违反协议，这种令牌交易的全局验证就没有发行者的验证安全。我们提出了一种新的令牌标准，称为TokenStrike[19]，其中每个令牌都使用一个由发行者签名的私有区块链来表示，这样几乎可以检测到发行者的任何不法活动，并证明该不法行为已经发生。TokenStrike旨在与HTLC兼容, 因此任何基于TokenStrike的令牌都可以交换为任何TokenStrike令牌或其他闪电网络资产。

8.2. 开放交易

另一个有前途的可扩展令牌交易技术是开放交易，它使用公证服务器池来验证代币或令牌交易，并使用多重签名对它们进行签名[20]。我们预计开放交易和TokenStrike项目将为去中心化宽带市场提供并行令牌发行解决方案。

8.3. RGB -彩色币

最后, 我们确定了彩色币作为一种可能代表宽带和路由器资源的方式。彩色币是少量的加密货币，令牌发行者可以通过声明赋予其特殊意义[21]。彩色币依赖于这样一个事实，即在非隐私的区块链中，彩色币币可以从一方追踪到另一方, 然而类似于基于以太网的令牌，它们需要全球验证才能进行交易。目前，RGB项目[22]正在研究允许使用闪电网络进行彩代币交易的技术。我们目前没有使用RGB的任何技术，但我们正在将其作为第三个可能的候选对象进行监控。

总之，我们相信近零成本令牌发行的问题是可以解决的，PKT网络将利用这些技术来构建一个去中心化带宽市场。基于在HTLCs上所做的工作，我们也相信，无论我们选择什么，令牌化的带宽和路由器资源都将能够快速地与支持区块链的任何其他HTLC上的资产进行原子交换，包括但不限于比特币、莱特币和以太币。我们希望出现一个完全去中心化的市场，不需要任何集中的监管机构或交易所来让参与者交换令牌化带宽、虚拟专用网络和路由器资源。

9. 总结

我们引入了PKT网络和PKT区块链，作为互联网扩展到核心数据中心之外的扩展解决方案。PKT网络是一个去中心化网络，它利用cjdns进行端到端加密，并利用技术进步来提高互联网路由和数据包传输效率。PKT网络架构激励边缘节点和云互联网服务提供商在边缘地带运营基础设施。PKT网络的免费层确保在资源未使用时，互联网访问始终可用。我们已经简要介绍了PacketCrypt协议，它创造了对带宽和PKT币的人为需求，为人们在边缘操作互联网基础设施提供了经济激励机制。我们描述了一个去中心化宽带市场，它将利用区块链技术进行结算、提供带宽租赁和市场传播。最后，我们介绍了路由设备，以进一步优化高速数据传输、加密和日常使用案例(如VPN)的先进性。这些创新巩固了PKT网络的相关性，以确保互联网接入、网络和数据通信都很便宜、易于访问和去中心化。

我们预计未来的互联网基础设施将由许多小型运营商拥有和运营，个人构成最大的群体，微型企业位居第二。基于卫星的互联网接入领域的创新可能会对全球互联网的可用性产生重大影响。然而，一些短距离通信链路，如与附近邻居家的wifi连接，总是比卫星通信更有效。对于横贯大陆和大陆间的通信，我们认为基于基础设施成本的降低, 卫星可能成为最有效的解决方案，但我们不能排除这样的可能性：随着技术的发展，地面屏蔽电缆将达到比自由空间通信更高的吞吐量。我们清楚地了解，一个去中心化带宽市场将是互联网发展的必要条件，并且对于PKT网络的开放协议和互操作性的需求将越来越大。

参考文献

[1] Woodcock, B. and Adhikari V. (2014). *Survey of characteristics of internet carrier interconnection agreements*. Packet Clearing House. https://www.pch.net/resources/papers/peering-survey/PCH-Peering-Survey-2011.pdf

[2] de Bijl, P., & Peitz, M. (2005). Local loop unbundling in Europe: Experience, prospects and policy challenges. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.690582

[3] Ford, G. S., & Spiwak, L. J. (2013). Lessons learned from the U.S. unbundling experience. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2378925

[4] Nardotto, M. (2016). Local loop unbundling in the UK does not affect broadband penetration - but it does lead to better service. *DIW Economic Bulletin*, 6(28), 311-317.

[5] Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet? : Illusions of a borderless world*. Oxford University Press.

[6] Munkholm, J. L. (2020). The pursuit of full spectrum dominance: The archives of the NSA. *Surveillance & Society*, *18*(2), 244-256. https://doi.org/10.24908/ss.v18i2.13266

[7] Shaw, I. G. R. (2016). *Predator empire: Drone warfare and full spectrum dominance*. University of Minnesota Press. https://books.google.com/books?id=Gil0DwAAQBAJ

[8] Bourreau, M., & Doğan, P. (2004). Service-based vs. facility-based competition in local access networks. *Information Economics and Policy*, *16*(2), 287-306. https://doi.org/10.1016/j.infoecopol.2003.05.002

[9] Briglauer, W. (2014). The impact of regulation and competition on the adoption of fiber-based broadband services: Recent evidence from the European Union member states. *Journal of Regulatory Economics*, *46*(1), 51–79.

[10] Hinden, M. R., & Haberman B. (2005). Unique local IPv6 unicast addresses, RFC 4193, *RFC Editor*, https://doi.org/10.17487/RFC4193

[11] *Cjdns project page*. https://github.com/cjdelisle/cjdns. 2020.

[12] *Pktd project page*. https://github.com/pkt-cash/pktd/. 2020.

[13] DeLisle, C. J., & Seesahai V. (2020, September 4). *PacketCrypt*. https://pkt.cash/PacketCrypt-2020-09-04.pdf

[14] Ofori-Attah, E., & Agyeman, M. O. (2017, January 25). *A survey of low power NoC design techniques.* Proceedings of the 2nd International Workshop on Advanced Interconnect Solutions and Technologies for Emerging Computing Systems, Stockholm, Sweden. https://doi.org/10.1145/3073763.3073767

[15] Sewell, K., Dreslinski, R. G., Manville, T., Satpathy, S., Pinckney, N., Blake, G., Cieslak, M., Das, R., Wenisch, T. F., Sylvester, D., Blaauw, D., & Mudge, T. (2012). Swizzle-switch networks for many-core systems. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, *2*(2), 278-294. https://doi.org/10.1109/jetcas.2012.2193936

[16] Xia, Y., Hamdi, M., & Chao, H. J. (2016). A practical large-capacity three-stage buffered clos-network switch architecture. *IEEE Transactions on Parallel and Distributed Systems*, *27*(2), 317-328. https://doi.org/10.1109/tpds.2015.2408614

[17] Herlihy, M. (2018, July 23-27). *Atomic cross-chain swaps*. Proceedings of the 2018 ACM symposium on Principles of distributed computing, United Kingdom. doi:10.1145/3212734.3212736

[18] *OpenDEX project page*. https://opendex.network/. 2020.

[19] *TokenStrike project page*. https://github.com/pkt-cash/ns-projects/blob/b0874ee/projects/2020_07_25_tokenstrike.md. 2020.

[20] Odom, C. (2015). *Open-transactions: Secure contracts between untrusted parties*. http://www.opentransactions.org/open-transactions.pdf

[21] Rosenfeld, M. (2012, December 4). *Overview of colored coins*. Bitcoil. https://bitcoil.co.il/BitcoinX.pdf

[22] *RGB project page*. https://rgb-org.github.io/. 2020.