独辟蹊径！“网络中立”作为区块链扩容解决方案

本文另辟蹊径，提出可验证中立云的概念，给出云分发网络解决区块链的可扩展性问题的思路，并探讨了如何验证云分发网络的中立性。

Author	Aleksandar Kuzmanovic
Translator	Taosheng Shi
WeChat Contact	data-lake
Mail Contact	tshshi@126.com
Document category	Distributed System & Blockchain
Document location	https://github.com/stone-note/articles

Version	Status	Date	Author/Translator	Description of changes
0.1	Draft	19/03/2019	Taosheng Shi	Initiate
0.2	Draft	DD-MM-YYYY	YourNameHere	TypeYourCommentsHere
1.0	Approved	DD-MM-YYYY	YourNameHere	TypeYourCommentsHere

译注：扩容、可扩展性、可伸缩性、性能等词语在区块链背景下是对同一问题的不同表述。

本文作者：Aleksandar Kuzmanovic 是美国西北大学计算机科学教授。他最近的研究包括内容交付网络、网络中立性和区块链。他是初创公司 bloXroute Labs 的联合创始人，并在该公司担任首席架构师。

Contents

由于区块链的去中心化特性（即没有一个实体控制其运行），越来越多的人们期待，或者至少是希望，区块链在更多领域发挥其颠覆性的潜力。然而，去中心化是有代价的：区块链无法规模化，无法及时处理大量甚至适量的交易。例如，比特币每秒处理三笔交易。

问题的根源，也是区块链的限制因素，在于区块链基于免信任（trustless）的对等网络模型。在这个模型中，信息必须在网络中的每一跳上传播和验证。毫无疑问，云分发网络可以解决其他领域的类似性能挑战(例如 Akamai 或 YouTube 解决 web 和视频的传输性能)，也可以用于解决区块链的可扩展性问题。问题在于，像云这样如此庞大的中心化基础设施扰乱了区块链的去中心化特性，从而消除了区块链的颠覆性潜力。由此，可以提出这样一个问题：***云分发网络能否在不破坏区块链去中心化特性的前提下提高其可扩展性？*** 答案是肯定的，解决方案的关键基于现有概念（网络中立）提出一个修改的高级版本：可验证中立云分发网络。

由比特币在 2008 年发起区块链和加密货币革命正在蓬勃发展。主流加密货币的市值虽然剧烈波动，但仍有数千亿美金的规模。区块链的一个独特特性是没有中心化治理。区块链依赖于第三方仲裁(即，一个由验证和认证所有交易的参与节点组成的全球对等网络)。基于区块链的纯粹分布式和去中心化设计，许多人认为，这种系统在加密货币之外的其他领域具有颠覆性的潜力，包括医疗、政府、制造、零售、保险、物联网、共享经济等。许许多多大大小小的高科技公司都在密切关注区块链领域，分析这项新技术将如何影响他们现有或未来的运营。

区块链的一个主要问题是可扩展性。区块链系统吞吐量是用系统能够支持的 TPS(每秒交易数)来度量的。比特币目前的平均吞吐量为 3 个 TPS，而 Visa 中心化系统的平均吞吐量为 2000 个 TPS，每日峰值为 4000 个 TPS，最大吞吐量为 5.6 万个 TPS。没有可扩展性，加密货币系统将很难成为主流，区块链也不太可能在任何其他领域实现其颠覆性潜力。

1 什么是区块链？

区块链是一个公共分布式账本，它存储所有过去的交易，本质上是一种类型的数据库，由对等网络中相互连接的多个(数万个)节点创建和共享。为了就数据库的正确副本达成共识，必须对写入数据库的某些规则加以规定。虽然规则可能有所不同，但一般包括以下内容：

- **交易**(通常将一定数量的加密货币从一个用户发送给另一个用户)必须包含来自参与节点的数字签名，以便进行身份验证。
- ***必须按顺序添加交易。***交易不会单个加入账本，相反，它们是成批添加的，称为区块。例如，比特币区块链要求每个新区块都包含一个哈希“难题”的答案，这个答案是由链上最后一个交易区块和正在添加的当前区块所唯一确定的。
- **向区块链添加区块既昂贵又需要竞争。**想要向区块链添加区块的各个参与节点要么投资加密货币，要么投资算力，例如，比特币需要的哈希“难题”。这样的参与节点称为矿工，向区块链添加新区块的过程称为挖矿。

- **最长的区块链是最新版本。**当这条规则与前面的规则相结合时，这使得成功伪造区块链的代价非常高。即使复制现有的区块链并试图修改最后几个区块，其代价也非常昂贵。一旦区块在网络上得到足够的确认，删除或修改区块在数学上就变得不可能。因此，交易只能添加到区块链，它们永远不会被删除。
- **独立验证。**当节点检查区块链数据库的副本时，它应该能够独立地验证前面的所有规则是否已被遵守。如果每个用户都能独立验证区块链，那么所有用户就可以就正确的区块链达成共识。
- **在区块链中添加区块可以收获报酬。**因为向区块链写入区块比较困难，所以并不是所有节点都会参与这个过程。许多用户会创建交易，然后要求将交易写入网络，用户通常会支付一定的费用作为矿工报酬。此外，只要矿工在一轮挖矿过程中获胜，并有机会在区块链中添加一个区块，他们就可以将新产出的加密货币分发给自己。
- **区块链发生分叉，通过最长链规则解决。**在区块链上达成共识不是立即的，有时区块链可能会出现分叉(数据库的不同副本)。分叉是区块链的公共账本在一段共同的历史之后发生分歧，账本的不同版本共存。节点通过选择网络上最长的区块链，可以解决分叉问题。

2 区块链可扩展性问题

在解释区块链可扩展性问题之前，让我们先看看它在现实中是如何表现的。图 1 和图 2 显示了比特币和以太坊这两种主流加密货币的交易积压情况。你可以看到，成千上万的交易定期等待区块链处理。为了增加被矿工选中"上链"的可能性，用户(自愿)增加了交易费。因此，交易费绝不是微不足道的，在交易拥堵期间，交易费可能会大幅增长。

FIGURE 1: **BITCOIN TRANSACTIONS BACKLOG**

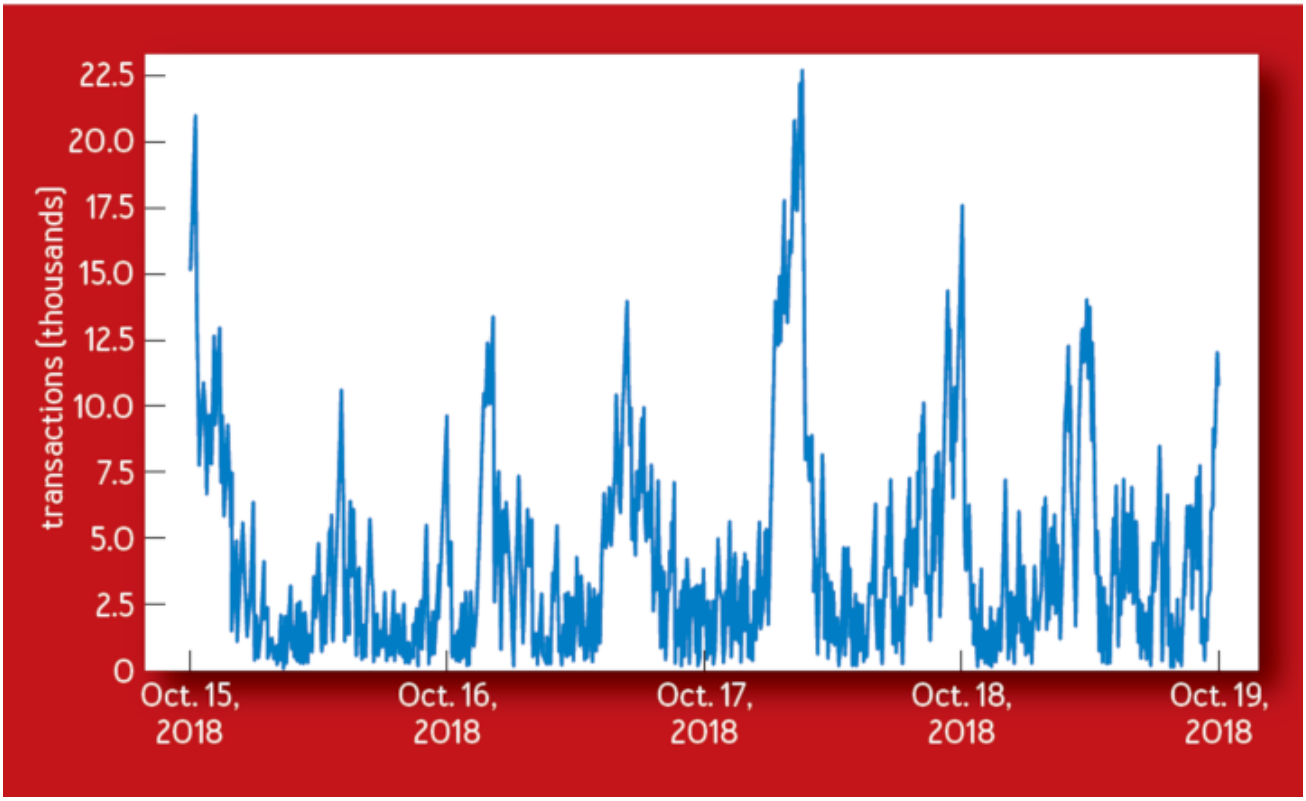
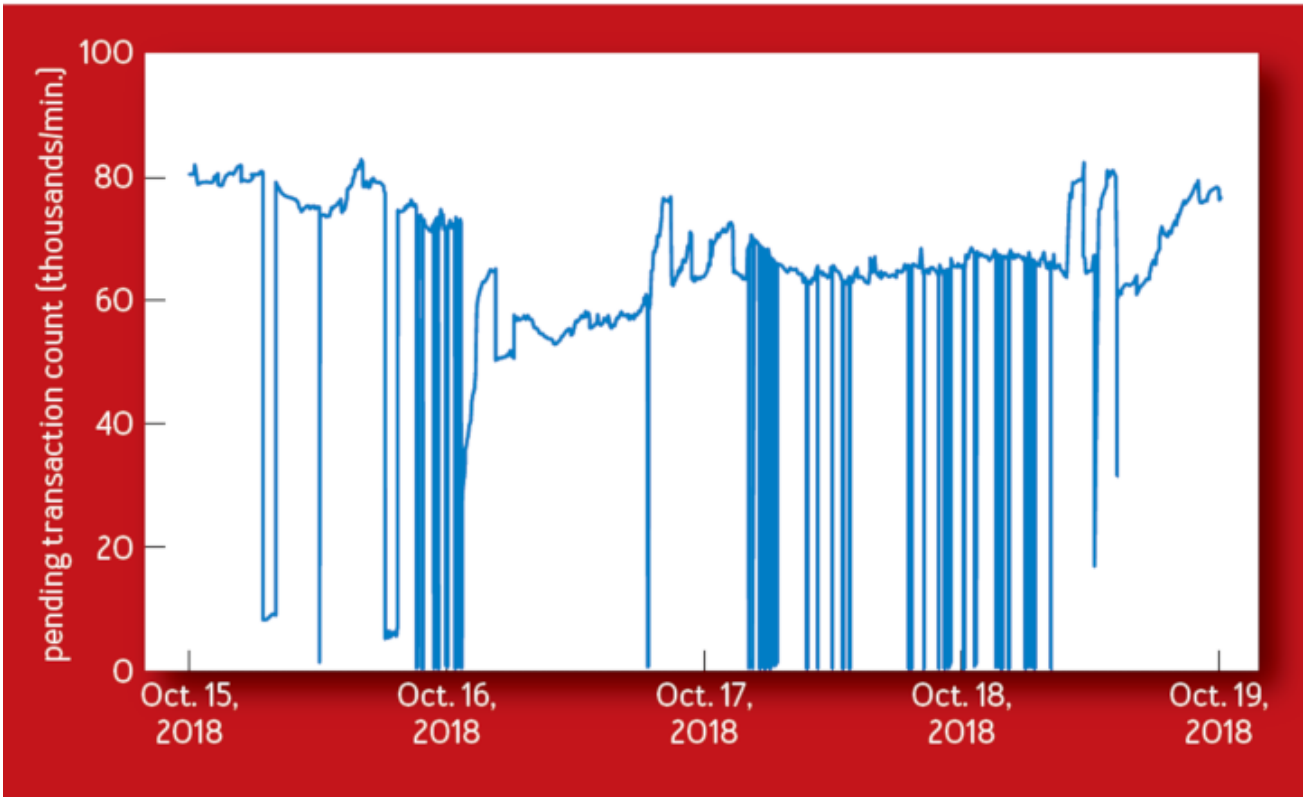


FIGURE 2: **ETHEREUM TRANSACTIONS BACKLOG**



为了理解瓶颈在哪里，让我们首先计算区块链吞吐量。系统吞吐量直接取决于两个参数：区块大小 B（即，每个区块中可以包含交易的字节数）和出块间隔时间 T（即，系统挖出一个新区块所需的平均时间）。在比特币中，B = 1 MB，T ~ 600 秒，大约是 3 个 TPS。由此，可以通过以下选项改进区块链的吞吐量：增加 B，以包含更多交易；减少 T，以更快的速度出块；或两者同时。问题是，这些参数都不能随意更改，稍后将详细介绍。

显然，正是区块链的分布式特性导致了这些问题。的确，只要区块和交易能够在节点之间瞬时传播，就可以快速地挖出大量区块，直到达到特定 CPU 和闪存阵列的限制。然而，实际上，区块链节点——成千上万甚至更多——分布在世界各地。***因此，网络是瓶颈。***

区块链网络中的节点以对等方式通信。不幸的是，这与以下高吞吐量、低延迟的目标背道而驰：

- 信息从一个节点传输到另一个节点；因此，在整个网络中传播信息需要多跳。由于网络中的每个节点都不信任其他节点，因此必须在每一跳独立地验证所传播的信息。这通常涉及在每个跳上执行加密操作，这会增加延迟并影响吞吐量。
- 区块链网络中节点的性能差异较大，这意味着关键路径上的单个慢节点会使传播时间膨胀。
- 最后，对等网络中的节点是随机形成的；因此，它们不是为了最佳数据传播而组织的。这意味着数据会通过网络中的次优路径传输。

因此，将一个 1MB 的区块传播到比特币网络 90%的节点平均需要 11.6 秒，这是 2017 年 3 月观察到的平均传播时间。不幸的是，这只是问题的一部分。在理论和实践中都表明，将区块大小 B 增加一个 X 因子也会使区块传播所需的时间增加相同 X 因子。同样地，将出块间隔时间 T 减少一个因子 X 也会产生完全对应的效果。这意味着区块传播时间随着这两个参数的增加而成比例地增加。

例如，将区块大小增加十倍也会将区块传播时间增加十倍，使它们的时间超过 100 秒。同样，将区块大小增加 100 倍将导致区块传播时间超过 1000 秒。这样的传播时间超过了出块间隔，导致每次挖出一个新区块时都会产生一个分叉。实际上，在这个场景中，不会通过继续挖出后续区块来解决分叉，相反，区块链将分解为”分叉“、”分叉的分叉“和”分叉的分叉的分叉“，直到节点和矿工不知道哪个分叉是“正确的”链——因此区块链崩溃。这是由网络瓶颈引起的区块链可扩展性问题。

3 云分发网络

云分发网络（Cloud-Delivery Networks）在解决 Internet 上的性能问题方面非常成功。这样的网络通过一个巨大的基础设施分发内容，这个基础设施可以由全世界成千上万的服务器组成(例如 Akamai)。此外，云分发网络执行广泛的网络和服务器测量，并使用这些测量结果将客户重定向到附近的服务器。这有助于互联网以巨大的规模运行。举个例子，单单 YouTube 就拥有超过 10 亿的用户，而北美晚上高峰时段高达 70%的网络流量来自 Netflix 和 YouTube 等流媒体视频和音频网站。如果没有云分发网络，这是不可能的。

这与区块链的现状形成了鲜明对比。实际上，正如前面所解释的，通过区块链网络传播一个 1 MB 的区块是一项耗时的任务，并且增加区块的大小可能会导致不可恢复的问题。然而，云分发网络每秒钟能够发送 TB 级的数据，这被认为是正常的。这样的网络可以用来扩展区块链吗？

毫无疑问，云分发网络可以提高区块链的性能。问题在于信任。在区块链生态系统中，节点不信任它的直连对等节点，***那么它如何信任一个比任何单个节点都强大得多的云分发网络呢？***云分发网络是可以审查区块链网络的交易、区块或矿工的中心化系统。例如，云分发网络管理员可以根据自己的政策、业务利益或法律要求，拒绝包含未经授权交易者的区块，或未经授权矿工的区块。

因此，关键的问题是，是否有可能让云分发网络变得免信任（trustless），这样它们就可以被用来扩展区块链网络，而无需行使本文前面提到的审查和其他权力。***这个概念被称为可验证网络中立（provable net neutrality）。***本文没有深入讨论其形式化定义，而是概述了与此概念相关的关键属性。

首先，网络不应该基于区块的内容审查信息。其次，网络不应该审查节点。第三，节点应该能够连续地验证上述两个属性，并且在网络出现错误行为时，可以放弃和替换网络。如何启用这些属性呢？

4 一个可验证的中立区块链分发网络

考虑一个云分发网络，它的目标是使区块链系统(不一定只是加密货币)能够扩展到每秒数千个上链交易。此外，它的另一个目标是同时为众多加密货币和区块链提供可伸缩性，使用全球基础设施以可验证的中立方式支持分布式区块链系统。这就是所谓的区块链分发网络 ***BDN（blockchain distribution network）***。本节概述了系统的信任模型，然后描述了实现中立属性所需的关键机制。

4.1 反向信任模型

区块链分发网络（BDN）的信任模型基于两个观察结果：首先，长时间的区块传播永远不可能大幅度提高免信任（trustless）区块链对等网络（如比特币）的可扩展性；其次，小型中心化系统可以很好地扩展，即通过信任一小部分参与节点并将区块链打包交易的控制权交给它们（例如 Ripple 和 EOS）。

然而，这种中心化破坏了区块链最显著的一个方面：对交易（或交易打包权）的分布式和去中心化控制。把区块链交易打包权交给有限数量的参与节点，这样就允许参与节点在用户、节点和矿工之间串通、审查和区别对待（discrimination）。有限的参与节点还降低了恶意节点为控制系统而不得不付出的节点数量代价。

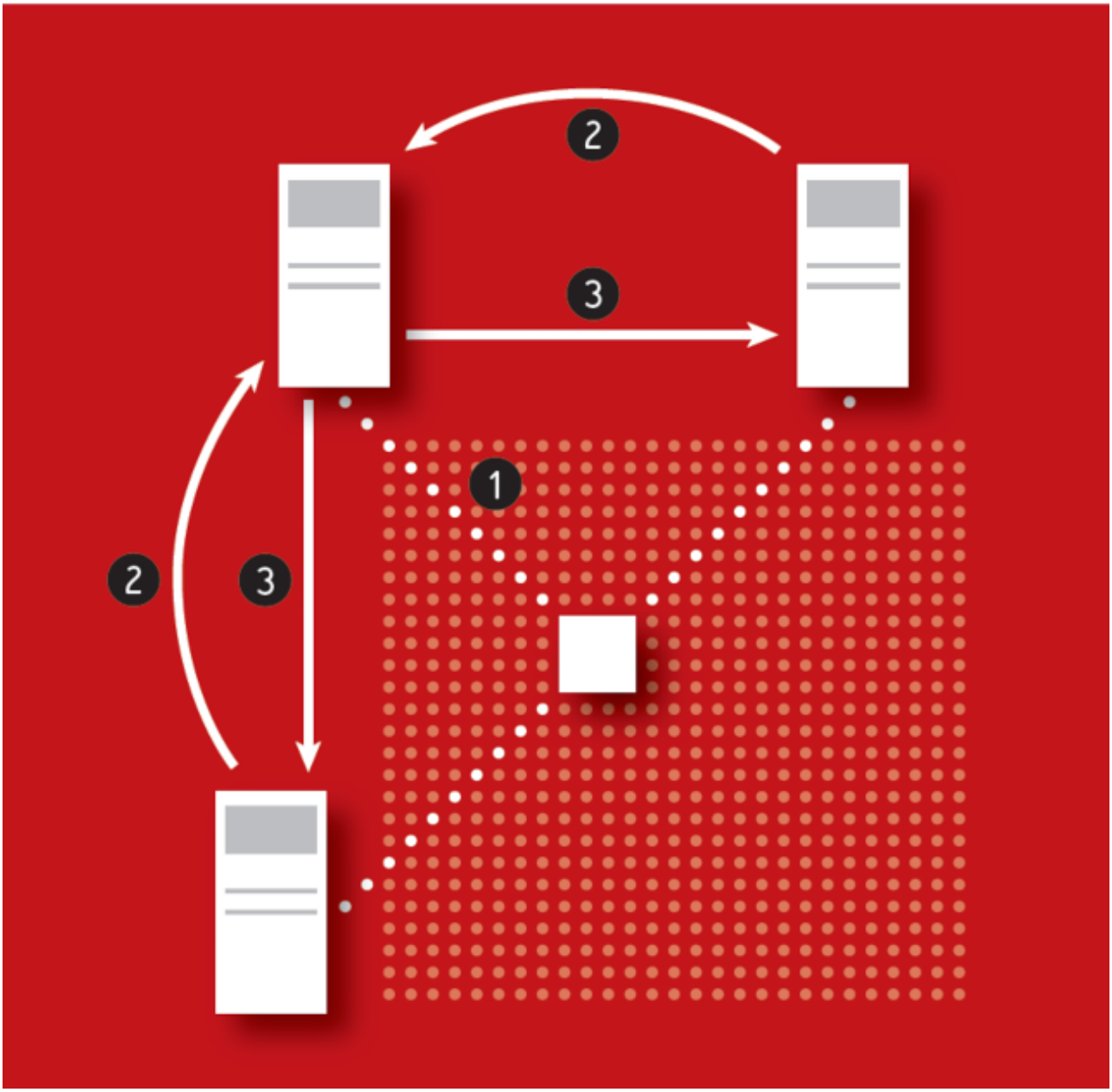
4.2 可验证网络中立

简而言之，区块链分发网络（BDN）只能将所有区块公平地传播给所有区块链节点，并且由于区块链节点的审计，BDN 无法区别对待区块（discrimination），仍然以点对点的方式连接。

4.3 加密区块

为了防止区块链分发网络（BDN）根据其内容阻止任何区块的传播，区块在加密后进行传播（图 3 中的步骤 1）。BDN 的加密还改变了区块大小，隐藏了交易的数量和它们的总大小。在区块被传播之后，接收方通过发送区块的哈希通知发送方（图 3 中的步骤 2）。最后，公布一个区块的加密密钥，并直接在区块链对等网络上传播（图 3 中的步骤 3）。加密密钥很小，只有几个字节，允许它在对等网络上直接快速传播，且 BDN 不能阻止它。

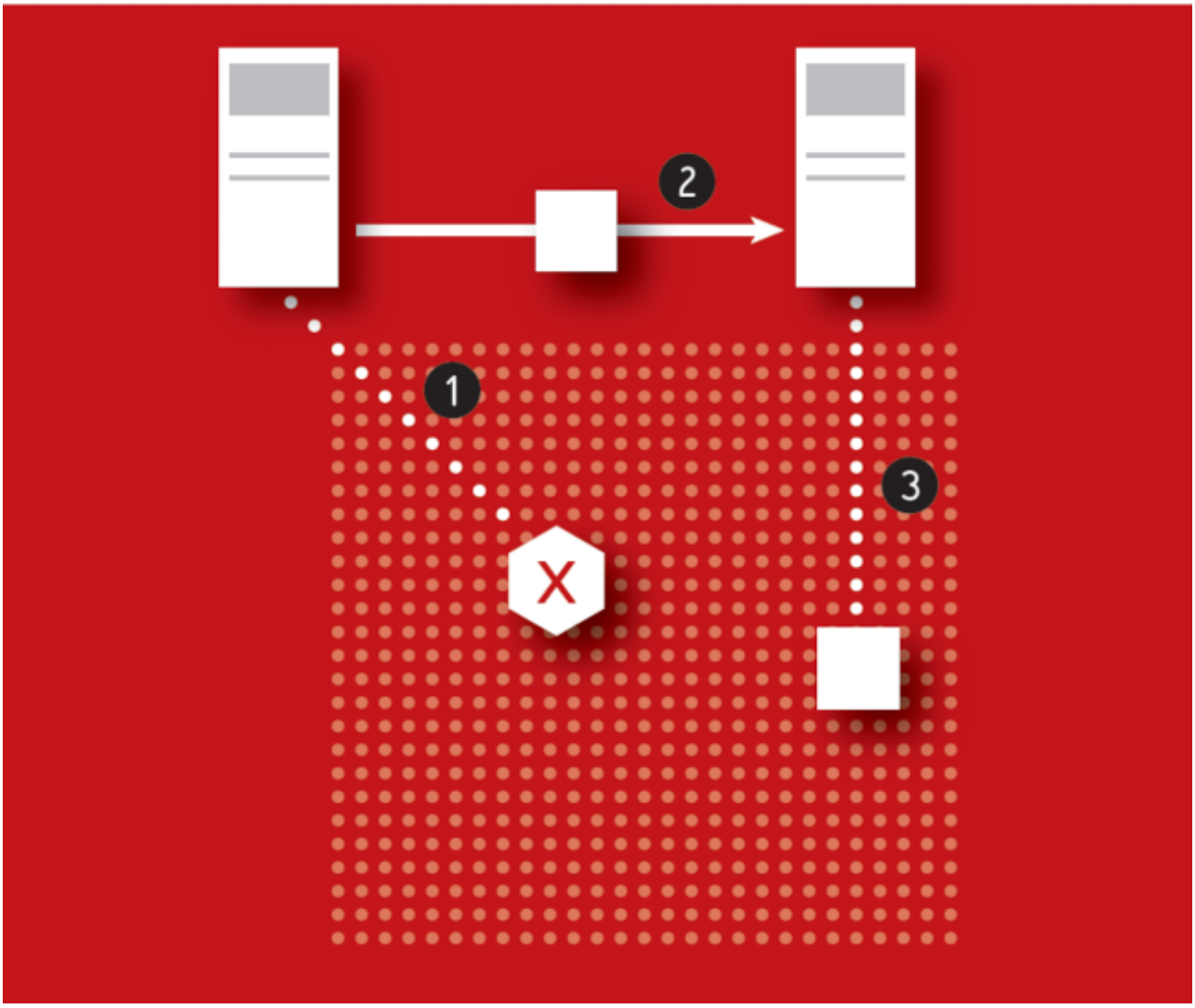
FIGURE 3: **ENCRYPTED BLOCK**



4.4 间接中继

为了确保区块链分发网络（BDN）不会阻止单个节点传播它们的区块，节点可以不将区块直接传播到 BDN。对于一个没有被 BDN 传播的区块(图 4 中的步骤 1)，发送节点将把它（区块）传播到对等网络上的一个对等节点(图 4 中的步骤 2)，这个对等节点将把它（区块）转发给 BDN(图 4 中的步骤 3)，对 BDN 混淆区块的起源。例如，在中国挖出一个区块的节点可以将其转发给欧洲的一个节点，然后该节点通过 BDN 发送该区块。除了间接地将区块中继到 BDN 之外，节点还可以请求它们的对等节点将来自 BDN 的传入区块中继给它们。这确保 BDN 不能通过延迟分发区块来区别对待节点，因为节点不需要为了从其服务中获益而与 BDN 直接交互。

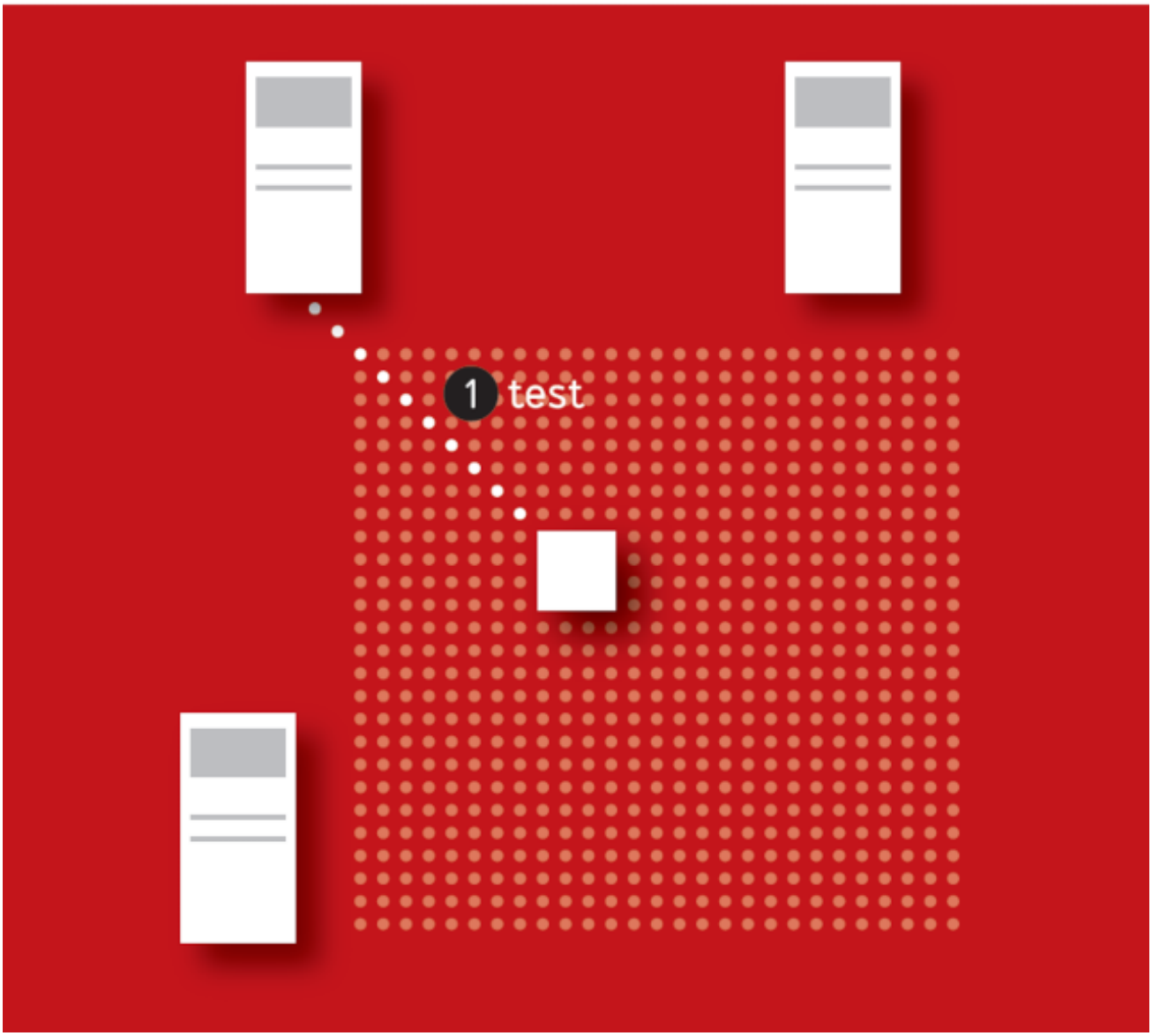
FIGURE 4: **INDIRECT RELAY**



4.5 通过测试区块进行审计

虽然区块链分发网络（BDN）不知道哪个节点挖到的区块，但它可能试图阻止或拖延来自某些节点子集的区块，从而影响它们所中继的所有区块。为了检测和防止这种行为，节点必须能够持续监视 BDN 的服务。这种监视是通过允许节点将加密的无效区块、测试区块直接发送到 BDN(图 5)并测量对等节点报告测试区块到达所需的时间来实现的。BDN 无法仅对有效区块使用歧视性策略，并忠实地传播测试区块，因为这两个测试区块在密钥发布之前是无法区分的。

FIGURE 5: **TEST BLOCK**



因此，通过使用流量加密和间接流量中继，以及显式审计 BDN，区块链节点能够限制 BDN 的不端行为，有效地将 BDN 管理员的权限与 BDN 基础设施解耦。如果 BDN 完全停止分发区块，或者只向一小部分节点分发区块，区块链节点可以放弃使用 BDN。

因为节点经常使用测试区块来推断接收区块的最佳来源，被 BDN 歧视的节点将只是从其对等节点接收区块。因此，如果 BDN 恶意歧视许多或所有对等节点，对等节点将简单地形成它们自己的对等网络，直到一个不同的系统取而代之。此外，如果歧视是由大规模的系统故障引起的，一旦故障得到解决，对等节点将返回使用 BDN。

5 性能

本质上，区块链分发网络（BDN）部署了广播原语，这意味着它可以有效地将数据从一个源节点传输到区块链网络中的所有其他节点。与对等网络相反（在对等网络中，每个区块链节点都连接到其他许多节点，这些节点通常分布在世界各地），区块链节点将这种一对多的通信替换为一对一的通信。这是因为区块链节点连接到单个 BDN 服务器。

对于较大的 TPS 速率，使用单个连接比使用多个连接更有助于提高可扩展性。为了有效地审计 BDN，必须在对等网络中连接区块链节点。然而，大部分数据是在 BDN 之间来回传输的。以下是 BDN 帮助扩展区块链的几种方法。

5.1 交易缓存

在区块链系统中，如比特币或以太坊，每个节点接收两次交易：第一次是原始交易，最初通过网络传播，第二次是将交易写入到区块中。BDN 可以有效地通过云分发交易，并对它们进行索引，然后在传输区块时利用索引(而不是原始交易)。这有效地将区块大小压缩了 100 多倍，假设原始交易大约 500 字节长，而索引可以是 4 字节或更少。

交易缓存是区块链生态系统中已经存在的一种思想，它已经被某些项目采用，但是它只被端点部署，而不是网络部署。因此，考虑到纯区块链系统中并非所有交易都到达所有端节点，即使是轻微的异步也会导致区块大小的显著增加（并不是所有的交易都是"压缩的"）；因此，性能会受到影响。相反，BDN 有效地传输和索引了区块链交易。

5.2 直通路由

与区块链节点不同，BDN 不能检查流经网络的区块的有效性，因为区块是加密的。这有助于通过网络快速传输数据块。特别是，在一个 BDN 节点接收到一个区块的所有比特之前，BDN 已经可以开始将接收到的区块的比特传输到网络的其他部分。这就是所谓的直通路由，它已经在网络交换机中被广泛采用了几十年。对于区块传播，它仍然可以显著加快数据传输速度，尤其是当数据块很大的时候。

5.3 交易 Incast 问题

交易需要在区块链网络中广播。在没有 BDN 的情况下，当 TPS 速率较高时，就会产生了所谓的交易 incast 问题：从多个源以较高的速率接收相同的交易。这将显著影响节点的资源，并影响整个区块链性能。BDN 消除了这个问题，因为大部分数据(包括交易)都是在单个 BDN 服务器之间传播的。

译者注：Incast is a many-to-one communication pattern commonly found in cloud data centers.

6 区块链可扩展性的相关研究

下面描述了提高区块链可扩展性的其他方法。

6.1 Off-chain 解决方案

提高可扩展性的另一种方法是使用 off-chain 交易，例如，闪电网络，其目的是减少主链上的冗余数据。一般来说，一个 off-chain 解决方案会在交易双方之间打开一个支付通道，即让买卖双方交换资金，同时记录中间结余，然后在区块链上进行交易结算。

BDN 提议对这样的解决方案不可知的（agnostic）。作为一个 off-chain 扩展解决方案，本质上仍然需要上链功能。此外，潜在的扩展效益是倍增的。如果底层的区块链能够支持比以前多 1000 倍的交易数量，并且 off-chain 交易将吞吐量增加 1000 倍，那么，区块链的吞吐量倍增了 6 个数量级。

6.2 On-chain 解决方案

On-chain 解决方案通常涉及以某种方式修改共识协议，以实现更高的吞吐量。其中一种方法，即分片技术（sharding），将区块链分割成几个较小的分片，一个全节点只需要追踪一个分片，而不是完整的区块链。这些分片相互交错，精心维护，以便保留区块链的原始安全属性。在这个领域还有许多其他的想法。虽然这些方法显示出一些潜力，但是它们的健壮性、安全性和可用性在实践中还有待观察。

尽管如此，在更快的网络层中，所有的 on-chain 解决方案都将执行得更好，这也是 BDN 提高其性能的地方。事实上，在每个分布式共识协议中，每个遵循协议的节点必须达成相同的决策。因此，每个这样的对等节点都必须独立于共识协议，获取关于系统中每个交易的信息。BDN 关注这个特殊的问题，这个问题本质上是一个广播问题，因为每个有效的信息片段都必须传播到系统中的每个对等节点。因此，BDN 对本地共识协议不可知的（agnostic），它能够显著提高任何区块链的性能。

7 总结

可验证中立云无疑是提高区块链可扩展性的可行解决方案。通过优化传输层，不仅可以从根本上提高吞吐量，而且可以显著降低延迟。事实上，当今数据中心的延迟分布已经偏向于大多数的微秒级，毫秒级只存在于分布的尾部。BDN 入网点没有理由不实现类似的性能。

在这些 BDN 入网点之间添加专用的光纤基础设施，将进一步减少吞吐量和延迟，从而建立高级 BDN 主干网。然而，实现这一愿景的关键在于通过区块链生态系统在底层网络基础设施中建立信任。这通过一个可验证中立网络设计将管理权限与基础设施解耦来实现。