BitTorrent 代币

摘要

TRON Foundation和BitTorrent Foundation将要推出名为BTT的新加密货币以及BitTorrent协议的扩展版本，以期在互联网上数亿台计算机上建立围绕社交、带宽和存储的代币经济。 我们最初的切入点是为现有的BitTorrent协议引入以代币为基础的优化方案，使网络参与者通过分享带宽和存贮所获得的价值突破现有水平的限制。 我们的长期愿景是拓展BitTorrent的使用范围，远远超出当前的用例，为第三方应用程序开发人员提供分布式基础架构平台，并使消费者能够从与他人分享其设备中闲置资源而获取少量价值。

我们项目的第一步是创建一个市场驱动的机制，使消费者能通过合作优化并延长现有BitTorrent文件共享组的寿命。 使用BitTorrent的附加插件，我们随后将为分布式应用程序开发人员提供机会，利用现有BitTorrent客户端提供的基础设施经验来发布新的应用程序，BitTorrent客户端已经具备了规模空前的分布式网络存储平台。 这些新应用程序将能够为用户提供激励（BTT），以换取访问经济高效的平台资源的权限，这些资源由极为广泛的已部署网络端点集合而成。 这些端点在互联网边缘的位置将对开发人员产生额外的吸引力，使得网络中立对手极难进行拦截。 最后，消费者在加密代币中获取其贡献的计算资源价值的能力将产生针对互联网消费者的全新交易机制，这不同于他们对某一事物的关注度或信用卡。

BitTorrent拥有超过1亿的月活跃用户，每周由数百万的新增安装数，它已经管理着互联网上最大的分布式计算生态系统之一。 通过整合BTT代币和交易处理，我们将解决BitTorrent的现有局限性，并开辟全新的无边界经济，在全球范围内交换计算资源的价值。 这将是对中本聪所著原版《比特币白皮书》发布十周年纪念日之际，对白皮书中愿景的实现和延伸。

TRON Foundation和BitTorrent Foundation是在新加坡共和国注册成立的法人实体。

背景

何为 BitTorrent？

BitTorrent是由Bram Cohen于2001年发明的一种开创性的分布式通信协议。 它是一种点对点协议，使用经济激励来使在互联网上传输容量大且需求量大的文件更容易，从而消除了人们对可信度高的中央服务器的需求。 它是一个开放式协议，已经独立执行了数十次，在过去16年中也被包含在软件中，这戏软件的下载和安装数达十亿次。 如今，该协议每月被超过1亿台连网的计算机定期使用。 该协议通过在开发者网站上审核的BitTorrent增强协议（BEP）的开放过程不断更新[1]。

BitTorrent 协议

BitTorrent 协议使客户端软件端点（即“客户端”）能够相互协作，从而将大文件高效且可靠地分发到多个客户端。 其做法是尝试同时有效地使用每个客户端上传和下载地带宽，以平衡整个“文件共享组”的合作客户端的点对点内容传输，并减少对任何单个弱点的依赖（比如与服务器的连接）。 理解协议如何运作的关键是了解底层的经济激励措施是如何实施的。

该协议基于一个系统，在该系统中，文件被切割成碎片，这些碎片在多个设备之间被交易，这些设备都试图同时获取该文件。 片段的加密哈希（“infohashes”）用于验证共享的片段确实是所请求的片段。 该系统基本上是物物交换经济的体现，其中每个客户端以交易其试图下载的文件片段的方式进行协作，而传输带宽是客户端决定与谁保持交易的决定因素。 各种机制通过进一步的交易奖励最有成效的物物交换，以断开交易甚至禁止交易方的手段来惩罚最低效的交易。 一旦客户端完成下载文件，尽管它不再有任何上传需要，出于回馈，如果它继续上传文件，它将被视为“种子”。大多数客户端的默认设置是“做种”给其他下载者，但此行为完全是利他的，下载完成后如果关闭BitTorrent客户端并停止做种也不会面临经济制裁。

[1] http://www.bittorrent.org/

BitTorrent 生态系统

BitTorrent协议已经执行了很多次，并且与坚持不同执行方式的公司和较受欢迎的志愿者维护版本之间保持健康的竞争。 除了执行BitTorrent协议的客户端软件外，还有一些基础设施提供商独立提供额外的有效服务（例如， 推荐端点和种子网站的跟踪服务器，在这些端点和站点中，用户可以索引被分享文件的元数据，并获得相关种子的访问权限）。 这向我们展现了一系列合作的分布式元素（客户端）和半分布式元素（中心服务器，种子文件站点）如何在积极性较高的攻击者的攻势下，成功维护存续时间长且高度活跃的生态系统。 在整合这个项目计划时，我们借鉴了在BitTorrent生态系统中学到的许多经验教训。

BitTorrent 公司

BitTorrent协议是世界上最大的去中心化协议，拥有超过10亿用户，远远超过排名第二的比特币（截至2018年10月21日，比特币总地址数为2944万[2])。 BitTorrent公司 发明并维护了BitTorrent协议。 虽然BitTorrent软件有诸多实现形式[3]，BitTorrent和µTorrent（通常称为“utorrent”）仍然是最受欢迎的两种。 2018年，BitTorrent协议与TRON波场区块链协议达成战略合作伙伴关系。 两者的合作使波场协议成为世界上最大的去中心化生态系统;它也使BitTorrent协议成为世界上最大的分布式应用程序。

BitTorrent公司管理的软件广受欢迎， 活跃用户遍及世界各地 由BitTorrent公司维护的软件客户端目前约有1亿活跃用户使用，每天新增安装数约为100万，每个国家几乎都有使用者， 超过160个国家拥有1万余名用户，而23个国家则拥有超过100万用户。 19个国家中有超过5%的互联网用户使用我们的软件（涵盖近6000万用户）。 此外，虽然还有其他BitTorrent软件提供商，但BitTorrent公司 的客户端产品目前占公共互联网上现有BitTorrent协议网络活动的40%[4]。

BitTorrent 和分布式应用程序

BitTorrent Foundation十多年来一直在探索分布式应用程序。 我们研究了BitTorrent协议的改编以及编写全新的协议，目的是提供一系列的服务：分布式消息传递，基于BitTorrent的CDN，点对点视频直播，文件同步和分布式网站等服务。

区块链技术的兴起实在振奋人心，也带来了可实现的范式转变，使得不信任方之间的协作能够持续比BitTorrent生态系统中可行性方案更长的时期。 但是，尽管许多新的去中心化协议都提出了雄心勃勃的技术路径，但在解决构建群聚效应这一巨大的市场挑战上，绝大多数协议都保持缄默，而这一点对所有分布式系统来说都是一项至关重要的技术必需品。 即使是个别几个为现有用户群引入加密代币的项目也不具备足够的经验，以微妙的手法设计一个能有效地平衡众多大规模经济利益的协议。 我们力求结合现有BitTorrent生态系统的群聚效应、BitTorrent 基金会的协议工程专长以及由波场TRON等平台开创的由区块链引入的新功能。

通过整合区块链技术来提供可靠且可扩展的存储和交换价值的机制，我们可以在现有的生态系统

[2] https://www.blockchain.com/charts/my-wallet-n-users
[3] ps://en.wikipedia.org/wiki/Comparison_of_BitTorrent_clients
[4] BitTorrent, Inc. 内部市场份额研究

之上启用新的分散式应用程序。 我们相信，扩展BitTorrent生态系统，与区块链技术结合，将使去中心化应用程序的开发人员能够在原有生态系统基础上构建，并帮助BitTorrent迎接一系列激动人心的新机遇。 我们认为，BitTorrent是迄今为止最接近能够引入基础设施以支持即将到来的分散式网络及其背后经济体系的技术用例。

项目起源

该项目是根据三个基本见解发展而来的：

1. 将去中心化的 BitTorrent 技术应用于许多新的用例，存在巨大且完全未实现的机会，而且市场现在比以往任何时候都更愿意这样做。
2. 如今，BitTorrent 协议的运行存在结构性低效率的问题，这限制了 BitTorrent 文件共享组的寿命，因此限制了其作为协议的整体有效性。
3. 大多数消费者（包括 BitTorrent 用户）都不愿意使用法定货币支付在线费用。 其必然结果是，人们用 “注意力” 来支付。这直接导致以隐私破坏信息垄断为主导的网络。

我们正在着手改进和扩展 BitTorrent，以通过与 BitTorrent 和区块链最佳技术相结合的项目来解决这些问题。

我们会将BitTorrent改造成一个为去中心化网络添砖加瓦的基础设施平台，让应用开发人员可以直接回馈为其提供底层资源的用户，并使得消费者可以用"寻得价值"与发布者和开发人员直接交易，无需使用法币。

为了加速引入，我们将首先解决 BitTorrent 当前工作中的低效问题。 这将激发基础技术的强烈吸引力，并提高消费者对该代币的存在，以及围绕其使用的用户体验和经济性的广泛熟悉程度。

同时我们将和第三方开发者合作，开发和推广各种 API 和分布式基础设施服务的市场。这样的 API 和市场建立在现有BitTorrent 技术中最根本的网络和存储基元之上。

我们还将与现有 BitTorrent 生态系统之外的第三方发布商和应用程序开发人员合作，共同开发消费者可能使用其代币的服务。

随着时间的推移，全球数以亿计的最终用户将拥有一种强大的新方法，可以从他们自己的技术资源中提取少量的价值，并有很多机会将这些价值用于他们选择的服务上。

高层面项目描述

我们将扩展 BitTorrent 协议，并引入一个名为 BitTorrent（BTT）的新 TRON TRC-10 加密代币，以实现分布式基础设施服务经济。 在这种经济环境中，最终用户可以以小增量提供基础设施服务以换取代币，并使用区块链解决方案来存储价值和交换媒介，以满足预期需求。

为了加快采用速度，我们将推出一项名为 BitTorrent Speed 的功能，以优化现有生态系统中 BitTorrent 的运行。 此功能的引入将解决BitTorrent中的问题，并证明使用基于区块链的奖励在大型的安装基础上以小增量提供基础设施服务的有效性。 我们将解决发布大规模以分布式帐本为基础的低延迟交易所带来的挑战。 最后，我们将概括 BitTorrent 客户提供的服务，并将其作为一个平台提供给外部应用程序开发人员。在此平台上可以启动未来的去中心化应用程序。

在下面的小节中， 我们将首先概述 BitTorrent (BTT) 加密代币。我们计划围绕它构建一种新的经济。 其次，我们将介绍区块链技术。交易处理将在其上运行。 第三，我们将概述优化现有 BitTorrent 协议的方法，称为 BitTorrent Speed。 第四，我们将描述如何使用 BitTorrent（BTT）代币操作 BitTorrent Speed。 第五，我们将讨论 BitTorrent (BTT) 服务的泛化，并描述在其基础上构建的一些首批去中心化应用程序。

BTT 加密代币和区块链

BitTorrent 现推出名为 BitTorrent（BTT）的 TRON TRC-10 加密代币，作为一种通用机制，用于交易 BitTorrent 客户端与任何其他参与服务请求者和服务提供者之间共享的计算资源。 BTT将是在支持BTT的BitTorrent生态系统中提供不同服务的主要交易单位。

BTT将作为可分割代币，允许对流动市场中服务请求者和服务供应商所提供的服务进行非常精细的定价。

BitTorrent Inc. 将部署一个“链上/链下交易所”，以促进高性能私有账本与波场公有链之间的代币转移。

BitTorrent Speed ™ - 提升共享网络寿命的激励措施

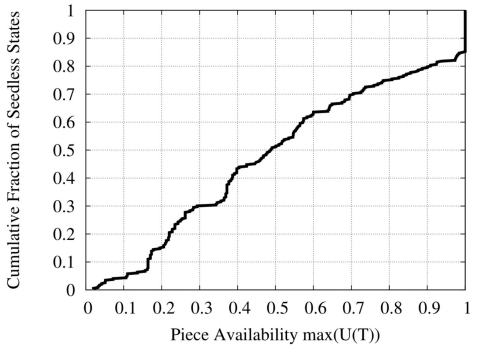
如前所述，BitTorrent共享文件组有结构性低效的问题，导致频繁的过早退化甚至夭折。 由于带宽不对称，文件完成下载通常比网络中一个端点上传等量字节要早很多。 一旦下载端点拥有了完整的文件，网络中没有足够的经济激励让其留下继续向其他下载者做种。 由于人们在离开文件共享组时提供的带宽没有他们贡献的多，许多 BitTorrent 文件群组不会持续多久。

在某些情况下，即使在没有种子的情况下，文件共享组也可以允许完成下载。 这种可能性在某些

客户端中被计算并显示为 "可用性" 度量[5]，通常表示为可用的分布式副本数量。 如果至少有一个活跃的非种子端点持有每个片段，则该文件被称为“可获得”。

BitTorrent协议包括了一个叫“最稀有优先”的设计决策。它规定当客户端要决定请求哪一个剩余未下载部分时，它应该优先请求所知且连上的端点持有量最少的文件部分。 该机制旨在使片段平均分布，以减少某一文件共享组失去提供某一必要片段的端点的可能性。

这两个考虑因素意味着种子不是完成下载的必要条件。 但研究表明，在大多数（约86%）无种案例中，这种集体重建是不可行的，而且做种者确实对文件的可获得性具有重大影响。[6]



图一， 来源：*解开BitTorrent文件的不可用性难题：测量与分析*

说白了, BitTorrent 整体功能已经相当不错了, 我们在此优化中提出的任何建议都不会逆转当前协议的运作方式。 我们也不建议以增加聚合分享行为为预期的优化，这种优化将向新加入者，也就是之前从未贡献种子的新人，增加共享行为。 我们想要增加的只是当前协议上的叠加， 它将允许BitTorrent文件共享组中的现有参与者更有效地相互分配资源。 为此，我们正在开发一种名为BitTorrent Speed的新功能，旨在使各端点能够为彼此提供基于加密代币的激励，以便在最初的下载完成后继续做种。

现有的BitTorrent易货市场将继续保持不变，但参与者需要在BitTorrent客户上运行一套新的BitTorrent协议插件，这样终端用户可以参与到包含BTT和上传速度的市场当中。

BitTorrent Speed功能将会被整合到未来的BitTorrent和µTorrent客户端中，使用户能够在（文件）共享组中宣传他们竞标的价格并交易BTT，以换取对种子的持续优先访问。 我们希望看到的结果是，端点将选择延长做种时间，从而为所有（文件）共享组参与者提供寿命更长的共享组和更快的下载速度。

我们实现BitTorrent Speed的方法始于BitTorrent当前分配资源的方式。 BitTorrent使用称为“投桃报李（tit-for-tat）”的共享算法，该算法通过名为“堵塞”的机制实现。 BitTorrent客户端将端点分为阻塞或未阻塞。 只有未阻塞的端点才能从客户端接收数据。 所有端点的阻塞状态定期（通常每15

[5] https://wiki.vuze.com/w/Availability
[6] *解开 BitTorrent 的文件不可用性：测量和分析* https://ieeexplore.ieee.org/document/5569991

秒）会被重新计算。 示例性阻塞算法可能根据自上次执行阻塞算法以来客户端从每个端点接收到多少数据来对端点进行排序。 然后，前 n 个节点被解除阻塞，其余的被阻塞。其中 n 是不堵塞通道的数量，是每个客户端执行的固定值。 种子文件不接收来自节点的任何数据，因此它们使用发送给每个节点的数据量。 这意味着种子文件优化以获得最大吞吐量，而不考虑公平性或其他任何问题。

还有许多不堵塞通道，通常是一个，它们则适用于另一个称为“乐观通阻（Optimistic Unchoking）”的阻塞算法。 乐观通阻（Optimistic Unchoking）算法以随机或循环方式选择节点解除阻塞。这使得新节点有机会接收一些数据，以便他们可以开始与其他节点互动。

阻塞是在BitTorrent（文件）共享组中分配资源的主要手段。 我们正是要改良这种机制，让客户端可以向他人提供奖励，以为他们自己想要得到的内容继续做种。 允许客户通过阻塞算法竞标BTT以获得优惠待遇，为他们提供了一个强大的工具，可以为种子在（文件）共享组的存续提供激励。

BitTorrent Speed 的运行说明

端点将同时作为服务请求者与服务提供者。 提供BTT以换取其他用户本地资源的端点是服务请求者，而提供此类资源服务服务以交换BTT的端点是服务提供者。

服务发现

当节点通过现有的 BitTorrent 协议机制发现彼此时，BitTorrent Speed 应用程序生命周期开始：它们使用哈希向中心服务器发布通告，或者在 DHT [7] 中找到给定哈希的节点。 通过这种方式，infohashes自然地将所有端点的空间划分为成不同群组的用户，这些用户在交换文件的片段时通常兴趣相投。

群中的潜在服务提供者是种子（具有完整的下载完成本地的种子副本的端点）或具有部分副本的端点。 这些服务提供者通过现有协议散播他们可提供部分 的 消息。

协议

初始余额

在客户的生命周期中首次竞标之前，服务请求者必须建立 BTT 余额。 要实现这一点，需要通过将一些 BTT 放入服务请求者和服务提供者之间的支付渠道。

首轮竞标

初始出价通过新的竞标 BitTorrent 协议扩展消息发送。发送给具有服务请求者所需要的一些片段的每个节点。 该消息包含服务请求者愿意为片段出价的 BTT 的数量。

宣布到中心服务器上

BitTorrent 中心服务器协议的扩展， 出价通告密钥，允许客户端在向中心服务器进行宣布时包含当前的出价。 该扩展添加了两个新的请求参数，允许客户端请求具有最高出价的节点。 由于宣布之间的间隔时间较长（30 分钟或更长），客户端不得信任中心服务器返回的出价。 如果节点的出价远低于中心服务器声称的出价，则客户端应断开该节点的连接。

第二个中心服务器协议扩展， 出价抓取，允许服务供应商检索哈希值列表，以及针对这些哈希值服务的最近出价。 这使得服务供应商能够以非常有效和去中心化的方式找到需要补充带宽的种子文件。

[7] 有关 BitTorrent 协议操作的详细说明，请参阅 https://en.wikipedia.org/wiki/BitTorrent

保留价格

客户端分享的每个种子文件都有与之相关的保留价格。 我们计划实施一种用户可配置的机制，其默认设计旨在使文件分享者所寻求的奖励随着时间的推移而增长。 当种子流完成后，默认的保留价格从0开始，然后在种子流被某已知端点最后一次占有的时刻开始随时间增长。 另一个节点的占有可以通过节点提交在种子文件中提供所选块的占有证明来证明。

当打开节点连接时，客户端发送包含底价和小块索引的底价消息。该小块可以发送其哈希，以证明另一个种子拥有该种子文件。 当保留价格或证据块更改时，保留价格消息也会发送在所有连接上。

可以在源证明消息中将拥有证明发送给客户端。该消息包含片段索引、块索引和块的哈希。 收到有效证据后，种子文件的底价将重置为零。

作为挑战来证明拥有某一片段的一小块应是客户端未在近期上传的块。 客户端为每个种子文件维护一个位图，其中每个位代表一个块。 当客户端上传块时，其相应的位设置为 1。 当种子文件的所有位变为 1 时，它们将被清零。 客户端通过获取伪随机数发生器（PRNG）的输出值来选择需要哪个块，该伪随机数发生器（PRNG）用与种子流的infohash异或的秘密值做种。 如果所选块的位置被设为1，则PRNG会被再次调用，直到所选块的位置是零为止。

自动竞价

对于初始版本，客户端将使用简化版的自动竞价机制。 在这个版本中，客户端单纯以钱包中BTT余额的一部分为竞标进行竞价。 出价计算方式如下：

竞标=（支出率）*BTT 余额/(剩余下载字节数 / 1024)

从这个公式可以看出，随着下载不断进行，竞标也会发生变化。 对于初始版本，客户不会重新竞标，除非竞标价格比之前的出价变化超过10%，且支出率（参数可以在0.0到1.0之间变化，具体取决于客户端竞标的积极程度））被定义为1.0。

将来，这个简单的算法将得到改进。 例如，客户端将可以根据现有的竞价信息流量和传输情况来预估未阻塞位置的市场价。 客户端通过正常的 BitTorrent 机制，也能知道各种下载片段的稀缺性。 如果客户端认为它们能够将稀有的片段发给出价更高的其他用户，客户端会选择自动竞价一定的数额。 这种基于激励的行为比起经典的“以牙还牙以眼还眼”，更接近于网络带宽拓扑。

竞价用户界面

竞价将在默认情况下自动进行。 用户的客户端将代表用户赚取代币，并且根据该用户的代币余额竞标。 我们可能会对用户公开界面控件，使得他们能够打开或关闭该功能，为某些种子文件打开或关闭竞价，调整支出率参数，设置保留价格，或对出价过程进行更精细的控制。

竞价修订和频率

由于客户端可能会收到低于其最高出价的数据（就目前在BitTorrent中的情况，免费的情况也时有

发生），通过将剩余总支出除以剩余数据计算的出价将随着时间的推移而向上爬升。 客户端可以实行任何它偏好的启发式来决定何时发送新的竞价信息，但发送新竞标的次数不能超过每分钟一次。 例如，客户端可以在初始竞标值变化超过10%的时候发送新的竞标。 如果用户更改了总BTT总额，那么客户理应立即发送新的竞价。

匹配

参与传统 BitTorrent 协议的用户主要根据从彼此那里接收数据的快慢来决定向哪些用户定期发送数据（也就是解阻） 我们扩展了这种unchoke机制，以便服务提供商在决定解阻哪个用户时同时考虑到竞价数据和用户上传率。 在具有BTT代币功能的客户端和传统 BitTorrent 客户端混杂的文件分享组中，服务请求者会向分享文件的人提出支付 BTT，但下载速度无论对方有没有提出给该文件支付 BTT 都会饱和。 这将会保留 BitTorrent的竞争性带宽市场。在这个市场中，不管另一个文件是否已有BTT定价，下载速度快的文件将会持续有效。

乐观解阻的位置不应与一般解阻的位置采用相同的拍卖形式。 在处理乐观解阻时必须小心谨慎，因为它们在允许新用户进入文件共享组方面具有重要作用。 如果客户端使用循环算法进行乐观解阻，那它只能在两个被阻塞时间相同的用户之间切断联系时实行竞拍。 在实际操作中，这意味着对于乐观解阻的位置进行竞拍只会发生在从未被解阻的竞标者之间。

当客户端运行上述的阻塞算法时，它首先产生一个列表，记录所有符合条件的竞标者。 如果该竞标等于或大于洪流的底价（如果价格可见），则被视为符合条件。

竞拍和阻塞的整合将根据客户端阻塞算法实施方法的不同而变化。 上述的算法示例可以改为先按照投标价格从高到低，再按接收数据从多到少排序。 当符合条件的投标者被解阻时，服务提供者首先给投标者发送一个新协议插件信息的投标回复。该回复包括竞标者应付的以BTT/byte计算的价格，以及发送BTT所必须的支付渠道的具体细节。 显示的价格必须小于或等于从竞标者那里收到的价格。 这条信息后面接的是正常的解阻信息。 如果中标者已经被解阻并且所需的价格已经改变，则在发送竞标回复和解阻信息之前，竞标者会先被阻塞，所有的请求也都会被拒绝。

客户可以使用他们喜欢的任何拍卖形式，但Vickrey-Clarke-Groves拍卖的变体是预计会产生最佳效果的那一种。 机制概述请见图2，这是一种多单位统一价格的拍卖。

每个服务请求者仅针对每个服务提供商的一个未解阻位置进行竞价。 因此，客户端将向每个未阻塞的投标人收取投标失败的最高费率，或所请求的种子文件的底价，以较高者为准。 如果只有一个投标人，则会收取底价。 这意味着投标人总是有一个基准激励来请求服务，在没有任何其他投标的情况下，他们将以底价获得服务，不管他们的出价是多少。

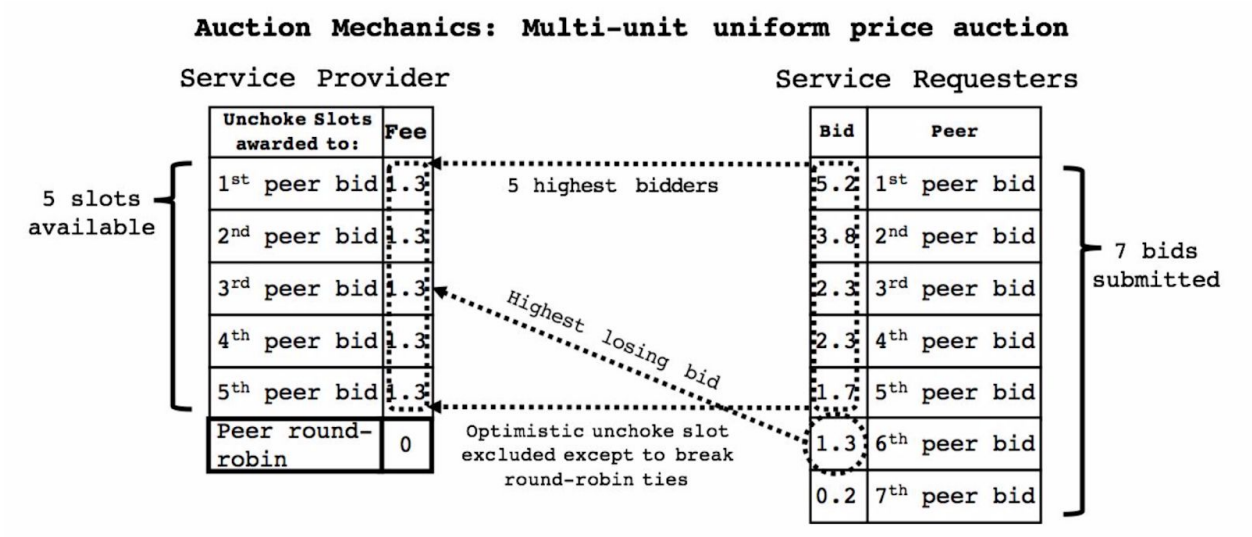


图 2

交易处理

一旦服务请求者收到解阻和竞价回复的信息，它就会以一个文件片段 BTT/字节速率的量向私有账本发送一份合同。

我们将客户端定义为发送BTT的一方，将文件分享者定义为接收它的一方。

1. 客户端创建公钥（K1）并向文件分享者（K2）请求公钥。 2. 客户端使用 OP_CHECKMULTISIG 创建并签署一个交易（T1）。该交易设置BTT /字节速率乘以所需字节数，以及需要文件分享者私钥和客户端密钥的输出。但是，此交易不会发送到付款渠道。 3. 客户创建一个连接到 T1 输出的退款交易（T2），该交易将所有资金返还给客户。 该交易在之后会被锁定一段时间，通常会比预期的下载时间还长几倍再加几个小时。 客户端不对其进行签名，并将这份未签名的交易提供给文件分享者。 一般来说，输出脚本为“2 K1 K2 2 CHECKMULTISIG”4。文件分享者使用和K2关联的私钥签署T2，并将签名返回给客户端。 需要注意的是，此时文件分享者还没有看到T1，只是看到了哈希值（在未签署的T2中）。 5. 客户端验证文件分享者的签名是否正确，若签名验证未通过，则过程终止。 6. 客户端签署T1并将签名传递给文件分享者，再由文件分享者将交易发送到支付渠道（如果双方都有渠道，则任何一方都可以进行这个操作）。 这就锁定了一定的BTT。 7. 然后客户端创建一个新的交易T3，它像退款交易一样连接到T1，并有两个输出口。 一个到K1，另一个到K2。 一开始，所有的数值都会被分配到第一个输出口（K1），与退款交易的操作完全相同，但时间上不会有锁定。 客户端签署T3并向文件分享者提供交易和签名。 8. 文件分享者验证输出值是否符合预期大小并验证

客户端所提供的签名是否正确。 9. 当客户端希望支付文件分享者，它会调整T3的副本，把更多价值分配给分享者，给自己分配少一些。 随后客户端重新签署T3并向文件分享者发送签名。它不需要发送整个交易, 只需要发送签名和所需增加的金额。 文件分享者调整其T3副本以匹配新数量，验证签名并继续。

这一直持续到传输结束，或者步骤3的超时即将结束。 然后文件分享者签署它看到的最后一笔交

易并将其发送到付款渠道，将最终金额分配给自己。 退款交易通常用以处理文件分享者消失或在某一时刻中止进程的情况，这使得分配价值悬而未决。 如果发生这种情况，那么一旦定时锁到期，该客户端就可以将退款交易发送到付款渠道并取回所有BTT。

锁定时间和序列号可以避免一种攻击，也就是当文件分享者提供片段，然后客户端使用TX2的第一个版本将输出双重花费，进而防止分享者领取BTT。 如果用户确实试图此种操作，TX不会立即被包括在内，为文件分享者提供一个时间窗口，在此期限内，它可以从支付渠道观察TX，然后发送它看到的最后一个版本，覆盖客户端试图进行的双花行为。

正常情况下，当服务请求者收到解阻消息时，服务提供者将开始发送片段。

如果由于某种原因在超时后传输没有完成，则服务请求者被阻塞并且不再接收数据。 服务请求者BTT转账再三失败可能导致服务提供商向服务请求者实施禁令。 被禁止的服务请求端点从网络中被断开，并且服务请求者的任何重新连接的请求在一段时间都会被拒绝。 同样，如果来自服务提供者的数据无法验证, 可能会导致服务提供商被禁。

各方逐步贡献带宽 (片断) 或 BTT, 并为流程中的每个步骤生成签名交易。 因此，服务提供商在任何给定时间的最大违规风险是与一个片段等值的带宽，并且由于服务请求者仅在验证交付时付费，因此他们没有违约风险。

广义BTT服务

优化现有的BitTorrent协议是引入加密货币大计中显而易见的第一步，但它对于将要实现的远景而言只是隔靴搔痒。 设置的先例即允许用户通过共享少量基础设施来存储价值，以便以后花费。 我们正在努力为具备BTT功能的BitTorrent客户端用户带去巨大的收入机会和消费机会。 针对营收机会，我们正在开发一系列广义BTT服务，并准备向第三方开发人员开放我们的平台，使得开发人员可以充分利用平台提供的服务，并以BTT支付。

通过与对我们平台感兴趣的合作伙伴进行广泛讨论，我们得出结论，首先会提供三种BTT服务：

（1）去中心化的内容传递服务，以使服务请求者能够宣传出价并为带宽支付BTT以接收特定片段内容。 此服务非常适合大规模内容分发，尤其是在存在审查员或其他类型的攻击者的情况下。 服务提供者将受到激励，以便为尽可能多的人提供可获取的内容，从而确保即使服务请求者数量庞大，强大性能也能得到保证。

（2）去中心化的存储服务，使服务请求者能够随时间支付存储费用。 服务提供者将同意存储一些数据并按需向服务请求者提供存储证明。 服务请求者还能够以预先计划的价格从服务提供者处下载存储的数据。 服务提供者将寻找随时间推移提供最高支付率的内容。 此服务对于远程备份和在小群组之间共享私有数据非常有用。

（3）去中心化代理服务，使服务请求者能够通过URL支付客户端来检索内容。 这对于高度移动化的应用程序或那些试图逃避IP级网络控制的应用程序非常有用。 该协议还将设计为允许以块的形式请求内容。 例如，这将允许具有间歇连接的客户端（例如依赖于wifi的移动用户）可靠地检索网络资源，而无需维持足够长的开放连接以接收完整内容。

随着新BTT应用程序的需求出现，更多BTT服务将会实现并引入服务提供者网络。 BitTorrent基金会将提供一个服务论坛以供大家讨论，并使新BTT服务标准化，一如其此前为BitTorrent协议所做的工作。

如图3所示，对BitTorrent协议的各项改善以及已概述的BTT交易处理方法空将被正式记录。 这些组成部分将作为去分布式应用程序的构成要素。

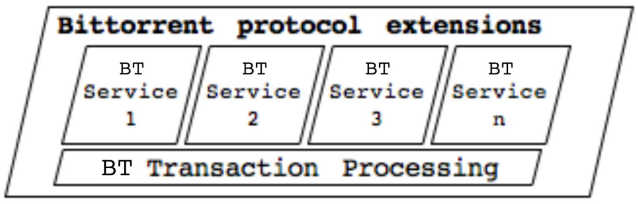


图 3

BitTorrent协议的扩展将提交至BitTorrent社区BEP流程获取评论 - BEP流程是一个非正式、但具有开放性的标准制定流程，[8] 由BitTorrent基金会推动，基金会在长达十几年的时期内一直为协议的改善提供指导。 我们会根据社区反馈，运用BitTorrent中完善的工程和发布管理实践来开发和测试这些扩展的应用。

此外，与我们处理极重要更新的常规做法一样，我们随后将把这些扩展作为开源库进行发布，并为第三方BitTorrent或其他客户端的集成建立支持和激励机制，以尽可能地拓展可支持BTT应用的客户端资源。

BTT激励措施

BitTorrent 生态系统在这种生产方向上的不断发展，将需要为广泛的现有和未来参与者提供协调和激励。 其他 BitTorrent 客户端实施者、第三方应用程序开发人员，以及其他在线发布者都有资格获得 BTT 激励奖励系统。

BitTorrent 生态系统多年来已经证明，如果数百万人能够安全和有保障地接受他们信任的协议的约束，他们将热情地分享他们的资源。 通过引入价值储存和交换机制，我们的目标是大大拓宽潜在参与者的范围----不论是服务请求者，还是服务提供者，或是两者兼而有之。 为了最大限度地提高成功率，我们必须确保BitTorrent公司 在启用BTT的BitTorrent生态系统中不是一个中心垄断者，就像它在当今的BitTorrent生态系统中远非垄断者一样。 这将需要协调各种活动，并向广泛的现有和未来参与者提供奖励。

图4所示的BTT项目证明生态系统合作伙伴的成功将为所有生态系统参与者带来回报的增加。

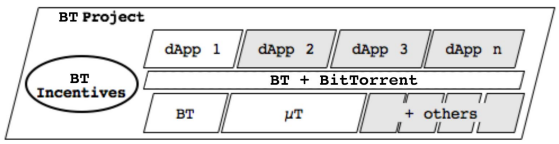


图4

BTT奖励的目的是：

[8] http://www.bittorrent.org/beps/bep_0000.html

- 向当前和潜在的参与者推广BTT项目，无论是服务提供者，服务请求者还是上述两者 - 这意味着要寻找并介绍有兴趣参与服务请求或服务提供的新应用程序开发人员; - 管理BTT生态系统参与者的成员资格和参与规则，其首要目标是建立一个公平公正的参与环境; - 以公平和透明的方式发放奖励和激励，这样

好的想法有机会脱颖而出，富有成效的结果可以得到公平的回报 - 与bittorrent.org上的志愿者一起工作，共同探讨未来

BitTorret协议的扩展。

一旦 BTT 项目以可持续的方式运行，我们可能会考虑将其为实施 BTT 激励而建立的规则和程序转变为较低开销的工具，例如中心化的自治组织（DAO）。 然而，第一件事，在不久的将来我们需要更多人的聪明才智和灵活变通，这就是为什么我们认为必须在BTT激励机制中加大投入（不管是人力还是代币）。

实施注意事项

区块链

BTT 应用程序将由每天数千万的活跃 BitTorrent 用户提供支持。 为了尽量减少欺诈机会，BTT 应用程序将以较小的增量提供服务，然后在提供更多服务之前等待确认付款。 这将需要在粒度级别处理交易，并在几秒钟内确认，最好在不到一秒的时间内进行确认。 此外，即使是我们对容量需求做最保守的估计，预计每秒也会有数十笔交易。 考虑到这些需求，现有的公共区块链显然将无法在短期内支持链上处理和结算。

用户控制

我们计划分阶段将 BitTorrent Speed 和 BTT 交易支持等功能引入 BitTorrent 和 µTorrent 客户端，以便我们能够迭代最清晰的用户教育之旅，从而优化最终用户的参与。 参与BTT交易的细节需要对终端用户保持完全公开，也给予他们完全的选择权，无论是参加或不参加。

BitTorrent 钱包

作为新推出的 BitTorrent 和 µTorrent 软件的一部分，我们将向所有用户分发集成的加密钱包，这些软件可以参与 BTT 应用程序。 由于我们将大规模分发这些钱包给大众市场的最终用户，而不一定是加密货币爱好者，我们需要密切关注其简单性和可用性。

引导：第一个可用的 BTT 应用程序将是 BitTorrent Speed 功能，该功能在一开始就未经过验证。考虑到新服务请求者的服务通常需要一段时间才能在大范围内普及，我们可能会另外一种战略，将一定数量的以营销为目的BTT代币播撒向市场。

BTT的用例多样化：以符合项目预期的规模范围引入BTT钱包，可能为从前未与BitTorrent技术有任何交集的新代币使用者创造机遇。 我们预计，数百万用户将能够积累少量实质价值不太高的

BTT，直到服务提供者们开始汇总这些代币。 这意味着通过提供服务而累积了少量BTT得用户将会寻找其他的途径来花费所得的代币，并且花费途径不仅仅是激励他人做种。 同时，我们希望能推广者中心能力，探索能促进商家接受这种新型未支付机制的合作伙伴关系。 这对于想要收集和使用代币的商家来讲是尤为有利的，为了支持其持续性的服务，商家需要用代币支付基础设施服务。

我们希望能够建立如图5所示的经济，其中BTT主要由分布式应用程序开发人员引入经济中，然后BTT在BitTorrent生态系统内外的服务请求者和服务提供者之间进行交易，并最终可能在具有商业重要性的服务提供者的池中聚集，这些提供者可能是BitTorrent生态系统的一部分，也可能不是。在本周期的当下，BTT将通过公开市场返回给新的服务请求者，他们希望用BTT交换为BitTorrent用户提供的分布式基础设施服务。

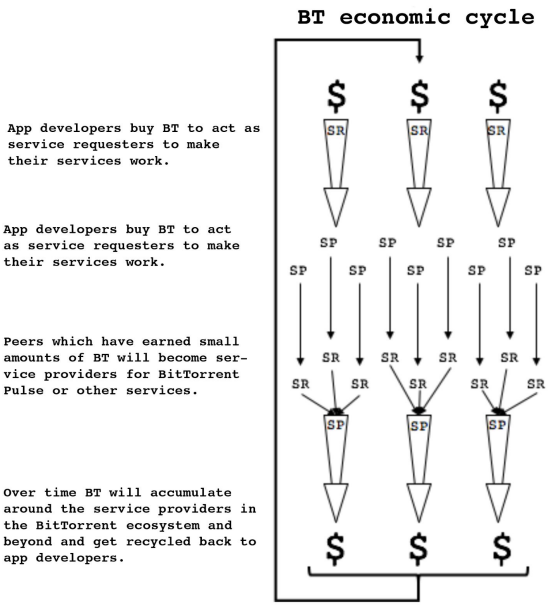


图5

身份：BitTorrent 作为一个协议，从未提供任何类型的身份服务，除了识别特定 IP + 端口号上的客户端之外。 也就是说，BitTorrent 实质上是识别在机器上运行的软件，而不是识别人。 这类似于加密货币背后的身份认证框架。 如果您可以访问存储代币的加密代币钱包软件，则通常认为它就是您的代币。 随着 BTT 的实施，我们希望遵循非常相似的方法来识别身份，并期望将 BTT 与客户端软件的参与片段紧密联系起来。 除了在该钱包上设置密码的可能性之外，目前我们不认为BTT项目将直接导致在BitTorrent中增加任何额外的新身份认证管理层的需要。

BTT 代币发行

我们发行的目标是：

我们将创建 990,000,000,000 BTT 的总供应量。 总供应量将按如下方式划分：BitTorrent公司的份额， 种子文件客户端用户安装和使用客户端的份额，既有TRX持有者的份额，第一批支持者和投资者的份额，BitTorrent基金会与团队份额，波场TRON基金会份额。

BitTorrent, Inc 种子文件客户端的用户（以及可能选择实施所需协议扩展的其他种子文件客户端）将能够提交 CAPTCHA 或工作量证明，这将允许他们访问 BTT 的初始余额。

结语

我们已经通过BTT项目--对BitTorrent的扩展--阐明了我们的动机，资质和计划，首先是旨在改善BitTorrent生态系统的新核心功能，新的加密代币，以及加密货币交易处理的大规模实际应用。

我们概述了如何推广这种方法，以使其他分布式应用程序开发人员能够使用具有超过1亿消费者的BitTorrent客户端组成的分布式基础架构平台来提供网络和存储资源，以换取BTT。 我们特别描述了来自独立应用程序开发人员的三个新颖的分布式应用程序，这些应用程序计划利用该平台并概

述他们在其中看到的价值。

我们已经描述了BTT激励计划的使命和运行，该计划将致力于推动BTT分布式应用数量不断增长，走向成功。 它也将更好的控制BTT向生态系统参与者逐步释放和分发BTT的过程， 在提升平台接受度方面功不可没。

我们已经讨论了一些重要的实施注意事项和挑战，以及我们计划解决这些问题的方案。

我们也制定了一份计划，阐明代币将如何发行并分享，以使得数百万计参与者所共享的计算机资源基础上的经济能走向稳定和繁荣。

该项目的潜力不仅仅是因为它将实现具有颠覆性的分散式应用程序，而且还因为其开放的生态系统方法将欢迎并奖励各个层级的参与者，另一个原因是BitTorrent生态系统在建设和部署分散的计算经济的显著先发优势。

参考

BitTorrent https://en.wikipedia.org/wiki/bittorrent_(software) BitTorrent 客户端 https://en.wikipedia.org/wiki/Comparison_of_bittorrent_clients BitTorrent 协议: https://en.wikipedia.org/wiki/bittorrent BitTorrent 公司: https://en.wikipedia.org/wiki/bittorrent_(company)

[*] BitTorrent.org：http：//www.bittorrent.org [*] BitTorrent.org BEP流程：http：//www.bittorrent.org/beps/bep_0000.html [*] BitTorrent 协议规范：http://www.bittorrent.org/beps/bep_0003.html

[*] BitTorrent.com: http://www.bittorrent.com [*] µTorrent.com: http://www.utorrent.com

[*] Libutp https://github.com/bittorrent/libutp [*]新开源 BitTorrent 协议旨在疏通管道 https://arstechnica.com/information-technology/2010/05/BitTorrent-open-sources-new-protocol-implementation/

[*] 解开 BitTorrent 的文件不可用性：测量和分析 http://ieeexplore.ieee.org/document/5569991/

附录

常见问题

为什么不重写 BitTorrent 协议？

像比特币这样的加密货币项目的成熟再次证明（如BitTorrent一样），分布式协议可以实现激励，允许大量互不信任的网络参与者进行高效协作。 与BitTorrent相比，比特币的新颖之处在于它引入了区块链概念，使得协作可以随着时间的推移愈久弥坚，不像BitTorrent网络中的协作是短暂的，并且发生在称为“（文件）共享组”这个完全独立和无关的事件中进行。 我们考虑对 BitTorrent 协议进行根本性重写，以允许协作持续一段时间，并确保“正确的分享行为”得到奖励。这样一来，更多长尾内容（只有偶尔需求的有价值内容）将会在更长时间内有效。 我们设想了一个协议，它既可以下载（比如 BitTorrent），又可以分发长期激励（比如比特币挖矿奖励）。 经过长时间的考虑，我们决定不采取这种方式了，有如下几个原因：

1. 问题的困难 - 在协议层面实施激励制度，需要对目标进行精确的思考。 我们发现不可能清楚地阐明长尾分享的目标应该是什么，以及如何避免欺骗 - 有很多 BitTorrent 文件共享组失败，因为没有任何人关注（例如，一个更好的文件版本出现） - 唯一可行的方案似乎是执行一个让消费者判断的投票系统，但这似乎有违将所有内容包含进协议的愿望。 简而言之，尝试以编程方式辨别应该和不应该保留的内容似乎是一个问题。我们在没有询问最终用户的情况下很难回答。 2. 需要严格优于现有的 BitTorrent（又名“软分叉而不是硬分叉”） - 任何协议重写都必须与现有的 BitTorrent 生态系统兼容 - 这会立即排除诸如惩罚不分享之类的行为 - 消费者只会选择使用实施 '旧' BitTorrent 协议的客户端。“旧”协议没有惩罚他们。 在现有的比特币空间内，与这一问题的相似之处在于，实施硬分叉的难度越来越大。 BitTorrent 生态系统现在如此之大，以至于硬分叉的成

功率极低。 3. 认为我们解决措施弄的过分复杂 - 可能需要人作为系统的中介（参与者投票）让我们坚信我们需要关注更简单的BitTorrent协议的拓展方式 - 设计一个建立在已有的加密货币基础上的投票机制。 这样做的好处是，允许市场确定应该分享什么，同时让 BitTorrent 增强而不改变其核心。

为什么在发明 BitTorrent 时没有包含激励机制？

事实上，早期对 BitTorrent 先行者项目的研究确实试图想象过如何管理持久激励机制。 他们失败的主要原因是难以找到有效的解决方案，在大规模运作的同时 “准确记录”。 使用加密代币的区块链和分布式账本解决方案提供了一种强有力的新方法来准确记录，以便即使在所有交易对方之间缺乏完全信任的情况下，也可以处理交易，并且可以大规模管理账本。

这个解决方案如何帮助我绕过网络中立对手？

几个例子：从IP到IP的代理将使用户找到被某个ISP阻止的内容，这是与一个站点与请求者都能连接上的中介相连实现的。

您将如何保护最终用户计算机免受恶意攻击？

终端用户的技术资源的使用将严格限制在仔细圈定的范围内所提供得网络或存储等技术服务。 网络连接将受到uTP的保护 - 一种自我调整的带宽机制，可确保应用程序在有任何其他应用程序（甚至在其他设备上）使用网络连接时进行节流。 存储将被加密并限制为用户可配置的最大值。 用户将能够配置他们接受哪些应用程序，以及不接受哪些应用程序。 BTT 服务的提供仅限于简单的基础设施操作，绝不允许不受信任的第三方在用户设备上执行代码。

用户可以选择退出吗？ 如果他们不想提供资源或赚取代币怎么办？

是的，用户将始终能够配置其共享的参数，或者在他们选择的情况下完全将其关闭。 该生态系统应该没有任何强制性要求。用户将保留因任何原因而选择退出的权利。