

Pi network 白皮书(中文版)

问题：第一代加密货币的可访问性

解决方案：Pi - Mining Goes Mobile

Pi 经济模型：平衡稀缺和获取

实用程序：在 p2p 中通过未利用的资源货币化

治理 - 为人民提供的货币

路线图/部署计划

2019 年 3 月 14 日的草案 1

前言

随着世界变得越来越数字化，加密货币是货币发展的下一个自然步骤。Pi 是日常人的第一种数字货币，代表着全球加密货币采用的重要一步。

我们的使命：建立一个由日常人员保护和运营的加密货币和智能合约平台。

我们的愿景：建立世界上最具包容性的点对点市场，由世界上使用最广泛的加密货币 Pi 推动

对于更高级读者的免责声明：因为 Pi 的使命是尽可能包容，我们将借此机会向兔子洞介绍我们的区块链新手:)

简介：为什么加密货币很重要

目前，我们的日常金融交易依赖于受信任的第三方来维护交易记录。例如，当您进行银行交易时，银行系统会保留记录并保证交易安全可靠。同样，当 Cindy 使用 PayPal 向 Steve 转账 5 美元时，PayPal 保留了从 Cindy 账户中扣除 5 美元的中央记录，并将 5 美元记入 Steve 的账户。银行，PayPal 等中介机构以及当前经济体系的其他成员在监管全球金融交易方面发挥着重要作用。

但是，这些可信中介的作用也有局限性：

1. 不公平的价值捕获。这些中介机构积累了数十亿美元的财富创造（PayPal 市值约为 130 亿美元），但几乎没有任何东西传递给他们的客户- 当地的日常人，他们的资金推动了全球经济的一个有意义的比例。越来越多的人落后了。
1. 费用。银行和公司收取大量费用以促进交易。这些费用往往不成比例地影响拥有最少替代品的低收入人群。

1. 审查制度。如果某个特定的可信中间人决定您不能转移资金，那么它可以限制您的资金流动。
1. 许可。可信赖的中间人充当可以任意阻止任何人成为网络一部分的守门人。
1. 假名。在隐私问题日益紧迫的时候，这些强大的看门人可能会意外地披露 - 或强迫您披露 - 更多关于您自己的财务信息，而不是您想要的。

比特币的“点对点电子现金系统”于 2009 年由一位匿名程序员（或团体）Satoshi Nakamoto 推出，是货币自由的分水岭。有史以来第一次，人们可以安全地交换价值，而无需第三方或可信中间人。用比特币支付意味着像 Steve 和 Cindy 这样的人可以直接相互支付，绕过机构费用，障碍和入侵。比特币确实是一种没有边界的货币，为新的全球经济提供动力和连接。

分布式分类帐简介

比特币通过使用分布式记录实现了这一历史性成就。虽然当前的金融体系依赖于传统的中心真实记录，但比特币记录由一个“验证者”的分布式社区维护，他们访问并更新了这个公共分类账。想象一下比特币协议是一个全球共享的“Google 表格”，其中包含由此分布式社区验证和维护的交易记录。

比特币（和一般区块链技术）的突破在于，即使记录由社区维护，该技术使他们能够始终就真实交易达成共识，确保作弊者不能记录虚假交易或超越系统。这种技术进步允许在不损害交易财务安全的情况下移除集中式中间人。

分布式账本的好处

除了权力下放，比特币或加密货币之外，还有一些不错的属性可以使货币更智能，更安全，尽管不同的加密货币在某些属性中可能更强，而在其他属性中则更弱，基于其协议的不同实现。加密货币存放在由公共可访问地址标识的加密钱包中，并由一个非常强大的私人密码（称为私钥）保护。此私钥以加密方式签署交易，实际上不可能创建欺诈性签名。这提供了安全性和不可见性。与政府当局可以扣押的传统银行账户不同，没有私钥的人永远不会将钱包中的加密货币带走。由于分散性，加密货币具有审查能力，因为任何人都可以向网络中的任何计算机提交交易以进行记录和验证。加密货币交易是不可变的，因为每个交易块代表之前存在的所有先前块的加密证明（散列）。一旦有人向您发送款项，他们就无法向您支付款项（即区块链中没有弹跳支票）。一些加密货币甚至可以支持原子交易。在这些加密货币之上构建的“智能合约”不仅仅依靠法律来执行，而是通过可公开审计的代码直接执行，这使得他们无法信任并且可能在许多业务中摆脱中间人，例如房地产的托管。

保护分布式账本（采矿）

维护分布式交易记录的挑战之一是安全性 - 具体而言，如何在防止欺诈活动的同时拥有一个开放且可编辑的分类账。为了应对这一挑战，比特币引入了一种名为“采矿”的新工艺（使用共识算法“工作证明”）来确定谁“信任”对交易的共享记录进行更新。

您可以将挖掘视为一种经济游戏，迫使“验证者”在尝试将交易添加到记录时证明其优点。要获得资格，验证者必须解决一系列复杂的计算难题。首先解决难题的验证者可以通过发布最新的交易块来获得奖励。发布最新的交易块允许验证者“挖掘”块奖励 - 目前 12.5 比特币（在撰写本文时约为 40,000 美元）。

这个过程是非常安全的，但它需要巨大的计算能力和能源消耗，因为用户基本上“烧钱”来解决赚取更多比特币的计算难题。刻度与奖励比率是如此惩罚，以至于在验证者的自身利益中始终将诚实交易发布到比特币记录中。

问题：权力和金钱的集中化使第一代加密货币无法实现

在比特币的早期，当只有少数人正在努力验证交易和挖掘第一块时，任何人都可以通过在他们的个人计算机上运行比特币挖掘软件来获

得 50 比特币。随着货币开始普及，聪明的矿工意识到，如果他们有多台计算机正在开采，他们可以赚更多钱。

随着比特币价值的持续增长，整个公司开始涌入矿山。这些公司开发了专用芯片（“ASIC”），并使用这些 ASIC 芯片构建了庞大的服务器场，以开采比特币。众所周知，这些巨大的矿业公司的出现推动了比特币淘金热，使得日常人员很难为网络做出贡献并获得奖励。他们的努力也开始消耗越来越多的计算能量，导致世界各地日益严重的环境问题。

比特币开采的便利性以及随后比特币矿业的兴起迅速在比特币网络中实现了生产力和财富的大规模集中化。为了提供一些背景信息，87%的比特币现在由 1%的网络拥有，其中许多硬币在早期几乎是免费开采的。另一个例子是比特币最大的采矿业务之一 Bitmain 已经赚取了[数十亿美元的收入和利润](#)。

比特币网络中的权力集中化使普通人非常困难和昂贵。如果您想获得比特币，您最简单的选择是：

1. 挖掘自己。只需连接专用硬件（如果您有兴趣，可以在[亚马逊](#)上找到[这个装备](#)！）然后去城里。只要知道，既然你将与来自世界各地的大型服务器农场竞争，消耗的能量与瑞士的国家一样多，你就无法开采多少

1. 在交易所买点比特币。今天，您可以在撰写本文时以 3,500 美元/币的单位价格购买比特币（注意：您可以购买小数量的比特币！）当然，您也会因为比特币的价格而承担相当大的风险非常不稳定。

比特币是第一个展示加密货币如何破坏当前财务模型的人，这使得人们能够在没有第三方的情况下进行交易。自由，灵活性和隐私的增加继续推动数字货币不可避免的进军成为一种新常态。尽管有其好处，比特币（可能是无意的）集中资金和权力对主流采用提出了有意义的障碍。Pi 的核心团队进行了研究，试图了解为什么人们不愿意进入加密货币领域。人们一直将投资/采矿风险列为进入的主要障碍。

解决方案：Pi - 在手机上实现挖掘

在确定采用这些关键障碍之后，Pi 核心团队开始寻找一种方法，允许日常人员挖掘（或获得加密货币奖励以验证分布式交易记录上的交易）。作为复习，维护分布式交易记录所带来的主要挑战之一是确保对此开放记录的更新不是欺诈性的。虽然比特币更新其记录的过程已被证实（燃烧能量/金钱以证明可靠性），但它并不是非常友好的用户（或行星！）。对于 Pi，我们引入了使用一致性算法的额外设计要求，该算法也非常用户友好，并且理想地允许在个人计算机和移动电话上进行挖掘。

在比较现有的一致性算法(将事务记录到分布式分类帐中的过程)时，恒星共识协议成为实现用户友好的移动优先挖掘的主要候选者。

[Stellar Consensus Protocol \(SCP\)](#) 由斯坦福大学计算机科学教授 David Mazières 设计，他也是 [Stellar Development Foundation](#) 的首席科学家。SCP 使用一种称为联邦拜占庭协议的新机制来确保对分布式分类账的更新是准确和值得信赖的。SCP 也通过自 2015 年开始运营的 Stellar 区块链在实践中部署。

共识算法的简要介绍

在开始介绍 Pi 一致性算法之前，有助于简单解释一致性算法对区块链的作用以及当今区块链协议通常使用的一致性算法的类型，例如比特币和 SCP。为清楚起见，本节以过于简化的方式明确写出，并且不完整。要获得更高的准确性，请参阅下面的“*适应 SCP*”部分，并阅读恒星共识协议文件。

区块链是一种容错的分布式系统，旨在完全排序一系列交易。容错分布式系统是计算机科学领域，已经研究了数十年。它们被称为分布式系统，因为它们没有集中式服务器，而是由分散的计算机列表（称为节点或对等体）组成，这些计算机需要就块的内容和总排序达成共识。它们也被称为容错，因为它们可以容忍一定程度的故障节点进入系统（例如，多达 33% 的节点可能有故障并且整个系统继续正常运行）。

共识算法分为两大类：选择节点作为产生下一个区块的领导者的类别，以及没有明确领导者但所有节点在交换选票后对下一个区块达成共识的共识算法。彼此发送计算机消息。（严格来说，最后一句话包含多个不准确之处，但它有助于我们解释广泛的笔画。）

比特币使用第一种类型的一致性算法：所有比特币节点在解决加密难题时相互竞争。因为解决方案是随机发现的，所以基本上是偶然找到解决方案的节点被选为产生下一个块的轮次的领导者。该算法被称为“工作证明”并导致大量能量消耗。

Stellar Consensus Protocol 的简要介绍

Pi 使用其他类型的共识算法，并基于恒星共识协议（SCP）和称为联邦拜占庭协议（FBA）的算法。这样的算法没有能量浪费，但是它们需要交换许多网络消息，以便节点对下一个块应该是什么达成“共识”。每个节点可以基于加密签名和交易历史独立地确定交易是否有效，例如进行转换和双重支出的权限。但是，对于一个计算机网络来商定在一个区块中记录哪些交易以及这些交易和区块的顺序，他们需要相互发信息并进行多轮投票才能达成共识。直观地说，*建议我们都投票给 A 块作为下一个*；“*我投票支持 A 区成为下一个区块*”；“*我确认我信任的大多数节点也投票给了块 A*”，共识算法使得该节点能够得出结论：“A 是下一个块；并且除了 A 之外可能没有任何区块作为下一个区块”；即使上述投票步骤看起来很多，互联网也足够快，而且这些消息都是轻量级的，因此这种共识算法比比特币的工作证明

更轻量级。这种算法的一个主要代表称为拜占庭容错（BFT）。今天的几个顶级区块链基于 BFT 的变体，例如 NEO 和 Ripple。

对 BFT 的一个主要批评是它有一个集中点：因为涉及投票，参与投票“法定人数”的节点集合由系统的创建者在其开始时集中确定。FBA 的贡献在于，每个节点不是具有一个集中确定的仲裁，而是设置它们自己的“仲裁片”，这将形成不同的法定人数。新节点可以以分散的方式加入网络：它们声明它们信任的节点并说服其他节点信任它们，但它们不必说服任何中央机构。

SCP 是 FBA 的一个实例。SCP 节点不是像比特币的工作证明一致算法那样燃烧能量，而是通过担保网络中其他节点值得信赖来保护共享记录。网络中的每个节点都构建一个仲裁片，由他们认为值得信赖的网络中的其他节点组成。仲裁基于其成员仲裁切片形成，并且当且仅当其仲裁中的一部分节点也将接受该事务时，验证器才接受新事务。由于整个网络的验证者构建了他们的法定人数，这些法定人数可以帮助节点就保证安全性的交易达成共识。您可以通过观看这个简短的 7 分钟[解释视频](#)或查看此信息来了解有关恒星共识协议的更多信息 [SCP 技术摘要](#)。

Pi 对恒星共识协议（SCP）的改编

Pi 的共识算法建立在 SCP 之上。SCP 已经正式证实[[Mazieres 2015](#)]，目前已在 Stellar Network 内实施。与主要由公司和机构(例

如 IBM)作为节点组成的 Stellar Network 不同 ,Pi 打算允许个人设备在协议级别上做出贡献并获得奖励 ,包括移动电话 ,笔记本电脑和计算机。以下是关于 Pi 如何将 SCP 应用于个人采矿的介绍。

作为 Pi 矿工 , Pi 用户可以扮演四个角色。即 :

- **先锋。** Pi 移动应用程序的用户 , 每天只是确认他们不是 “机器人”。该用户每次登录应用时都会验证其存在。他们还可以打开应用程序来请求交易 (例如在 Pi 中向另一位先锋付款)
- **贡献者。** Pi 移动应用程序的用户通过提供他或她知道并信任的先驱者列表来做出贡献。总的来说 , Pi 贡献者将构建一个全局信任图。
- **大使。** Pi 移动应用程序的用户 , 他将其他用户引入 Pi 网络。
- **节点。** 作为先锋的用户 , 使用 Pi 移动应用程序的贡献者 , 并且还在他们的台式机或笔记本电脑上运行 Pi 节点软件。Pi 节点软件是运行核心 SCP 算法的软件 , 考虑了贡献者提供的信任图信息。

用户可以播放多个上述角色。所有角色都是必要的 , 因此只要他们在那一天参与并贡献 , 所有角色每天都会获得新创建的 Pi 奖励。在一个 “矿工” 的松散定义中 , 作为一个用户 , 他将收到的新货币作为捐款的奖励 , 所有四个角色都被认为是 Pi 矿工。我们比其传统意义更广泛地定义 “挖掘” 等同于执行比特币或以太坊中的工作证明共识算法。

首先，我们需要强调 Pi Node 软件尚未发布。因此，本节更多地作为架构设计提供，并作为征求技术社区意见的请求。该软件将是完全开源的，它也将在很大程度上依赖于 stellar-core，这也是开源软件，可[在此处获得](#)。这意味着社区中的任何人都可以阅读，评论并提出改进建议。以下是 Pi 提议对 SCP 进行的更改，以便通过单个设备进行挖掘。

节点

为了便于阅读，我们将*正确连接的节点*定义为 SCP 论文所指的*完整节点*。此外，为了便于阅读，我们将*主要的 Pi 网络*定义为 *Pi 网络*中所有完整节点的集合。每个节点的主要任务是配置为正确连接到主 Pi 网络。直观地，未正确连接到主网络的节点类似于未连接到主比特币网络的比特币节点。

在 SCP 的术语中，要使节点正确连接，意味着该节点必须选择“仲裁片”，以便包含此节点的所有结果仲裁与现有网络的仲裁相交。更确切地说，一个结点 V_{n+1} 被正确地连接到主网络 N 已经正确连接的 n 的节点 (V_1, V_2, \dots, V_n) 如果所得到的系统 N'_{n+1} 个节点 $(V_1, V_2, \dots, V_{n+1})$ 享有法定人数相交。换句话说，如果任何两个法定人数共享一个节点， N' 享有法定人数相交。-即，对于所有法定人数 U_1 和 U_2 ， $U_1 \cap U_2 \neq \emptyset$ 。

Pi 对现有 Stellar 共识部署的主要贡献在于它引入了 Pi 贡献者提供的信任图的概念，作为 Pi 节点在设置其配置以连接到主 Pi 网络时可以使用的信息。

在选择仲裁片时，这些节点必须考虑贡献者提供的信任图，包括他们自己的安全圈。为了帮助做出这一决定，我们打算提供辅助图形分析软件，以帮助运行节点的用户做出尽可能明智的决策。该软件的日常输出包括：

- 按照与信任图中当前节点的距离排序的节点排序列表；节点的排名列表基于 [PageRank](#) 的节点的信任图分析
- 社区报告的节点列表，以任何方式出现故障，寻求加入网络的新节点列表
- 网上关于“行为不端的 Pi 节点”和其他相关关键词的最新文章列表；包含 Pi 网络的节点的可视化表示，类似于 [StellarBeat Quorum 监视器](#)中显示的 [[源代码](#)]
- 与 [QuorumExplorer.com](#) 类似的仲裁浏览器 [[源代码](#)]
- 像 [StellarBeat Quorum 监视器](#)中的模拟工具，它显示当前节点的配置发生变化时，此节点与 Pi 网络的连接所产生的预期影响。

未来工作的一个有趣的研究问题是开发可以考虑信任图的算法，并建议每个节点的最佳配置，甚至自动设置该配置。在 Pi 网络的第一次部署中，运行节点的用户可以随时更新其节点配置，系统将提示他们每天确认其配置，并在他们认为合适时要求更新它们。

移动应用用户

当 Pioneer 需要确认某个特定交易已经执行时（例如他们已经收到 Pi），他们就会打开移动应用程序。此时，移动应用程序连接到一个或多个节点以询问交易是否已记录在分类帐上，并且还获取该块的最新块编号和散列值。如果 Pioneer 也在运行 Node，那么移动应用程序将连接到 Pioneer 自己的节点。如果 Pioneer 未运行节点，则应用程序将连接到多个节点并交叉检查此信息。先锋将有能力选择他们希望他们的应用程序连接到哪些节点。但是为了使大多数用户变得简单，应用程序应该具有合理的默认节点集，例如基于信任图最接近用户的多个节点，以及随机选择的高页面节点。

挖掘奖励

SCP 算法的一个美妙特性是它比区块链更通用。它协调分布式节点系统的共识。这意味着相同的核心算法不仅每隔几秒用于在新块中记录新事务，而且还可用于定期运行更复杂的计算。例如，每周一次，恒星网络正在使用它来计算恒星网络上的通货膨胀，并按比例分配所有恒星硬币持有者（Stellar 的硬币称为流明）。以类似的方式，Pi 网络每天使用一次 SCP 来计算在任何特定日期积极参与的所有 Pi 矿工（先驱者，贡献者，大使，节点）的全网新 Pi 分布。换一种说法，

为了比较，比特币在每个区块上分配采矿奖励，并且它给予矿工足够幸运能够解决计算密集型随机任务的所有奖励。比特币目前的 12.5

比特币（约 40,000 美元）的奖励每 10 分钟只给一名矿工。这使得任何给定的矿工都不可能获得奖励。作为解决方案，比特币矿工在集中式采矿池中组织起来，这些采矿池都有助于提高处理能力，增加获得奖励的可能性，并最终按比例分享这些奖励。采矿池不仅是集中化的重点，而且它们的运营商也会削减开采量，减少个别矿工的数量。在 Pi 中，不需要采矿池，因为每天都有一次贡献得到新 Pi 的精英分布。

交易费用

与比特币交易类似，Pi 网络中的费用是可选的。每个块都有一定的限制，可以包含多少个事务。当没有积压的交易时，交易往往是免费的。但是如果有更多的交易，节点会按费用对它们进行排序，最高费用交易位于顶部，并且只选择要包含在生产的块中的最高交易。这使它成为一个开放的市场。实施：每天一次在节点之间按比例分摊费用。在每个街区，每笔交易的费用都会转移到一个临时钱包中，从那里最终分配给当天活跃的矿工。这个钱包有一个未知的私钥。

限制和未来的工作

作为 Stellar Network 的一部分，SCP 已经进行了多年的广泛测试，在撰写本文时，它是世界上第九大加密货币。这给了我们很大的信心。Pi 项目的一个目标是将 Pi 网络中的节点数量扩展为大于 Stellar 网络中的节点数量，以允许更多日常用户参与核心一致性算法。增加节点

数量将不可避免地增加必须在它们之间交换的网络消息的数量。即使这些消息比图像或 YouTube 视频小得多，并且今天的因特网可以可靠地快速传输视频，但是必要的消息数量随着参与节点的数量而增加，这可能成为达成共识的速度的瓶颈。这最终会降低网络中记录新块和新事务的速率。值得庆幸的是，Stellar 目前比比特币快得多。目前，Stellar 已经过校准，每隔 3 到 5 秒生成一个新块，每秒可以支持数千个事务。相比之下，比特币每 10 分钟产生一个新的块。此外，由于比特币缺乏安全保障，比特币在极少数情况下的区块链可在第一个小时内被覆盖。这意味着比特币的用户必须等待大约 1 小时才能确定交易被认为是最终的。SCP 保证安全，这意味着在 3-5 秒之后就可以确定交易。因此，即使存在潜在的可扩展性瓶颈，

虽然 SCP 的可扩展性仍然是一个开放的研究问题。有许多有希望的方法可以加快速度。一种可能的可扩展性解决方案是 [bloXroute](#)。BloXroute 提出了一种区块链分发网络 (BDN)，它利用针对网络性能优化的全球服务器网络。虽然每个 BDN 由一个组织集中控制，但它们提供可证明中立的消息传递加速。即 BDN 只能在没有歧视的情况下公平地为所有节点提供服务，因为消息是加密的。这意味着 BDN 不知道消息来自何处，它们去往何处或内部是什么。这样，Pi 节点可以有两个消息传递路由：一个快速通过 BDN，预计大部分时间都是可靠的，它的原始对等消息传递接口完全分散且可靠但速度较慢。这个想法的直觉与缓存模糊地类似：缓存是计算机可以非常快速

地访问数据的地方，加快了平均计算速度，但不能保证始终拥有所有必需的信息。当缓存未命中时，计算机速度变慢但没有发生灾难性事件。另一种解决方案是在开放的点对点网络中使用多播消息的安全确认[Nicolosi 和 Mazieres 2004]加速同伴之间的信息传播。

Pi 经济模型：平衡稀缺和获取

第一代经济模型的利弊

比特币最令人印象深刻的创新之一是分布式系统与经济博弈理论的结合。

优点

固定供应

比特币的经济模式很简单。现在只有 2100 万比特币。此编号在代码中设置。世界各地的 7.5 亿人中只有 21 亿人流通，没有足够的比特币可供使用。这种稀缺性是比特币价值最重要的驱动因素之一。

减少块奖励

比特币的分销方案如下图所示，进一步强化了这种稀缺感。比特币区块采矿奖励每 210,000 个区块减半（大约每隔 4 年。）在早期，比特币区块奖励为 50 个硬币。现在，奖励是 12.5，并且将在 2020 年

5 月进一步减少到 6.25 个硬币。比特币的分配率下降意味着，即使货币意识增强，实际开采的数量也会减少。

缺点

倒置意味着不均匀

比特币的倒置分布模式（开始时收入增加的人越少，今天人们收入越少）是其分布不均的主要原因之一。由于一些早期采用者掌握了如此多的比特币，新矿工正在为更少的比特币“燃烧”更多的能量。

囤积抑制用作交换媒介

尽管比特币是作为“点对点电子现金”系统发布的，但比特币的相对稀缺性阻碍了比特币作为媒体交易所的目标。比特币的稀缺性导致其被视为“数字黄金”或数字存储价值的形式。这种看法的结果是许多比特币持有者不愿意将比特币花在日常开支上。

Pi 经济模型

另一方面，Pi 试图在为 Pi 创造稀缺感之间取得平衡，同时仍然确保大量不会累积到极少数人手中。我们希望确保我们的用户在为网络做出贡献时获得更多的 Pi。Pi 的目标是建立一个足够复杂的经济模型，以实现和平衡这些优先级，同时保持足够直观，供人们使用。

Pi 的经济模型设计要求：

- **简单**：构建直观透明的模型
- **公平分配**：让世界人口的临界质量进入 Pi

- **稀缺性**：随着时间的推移，创造一种**稀缺**感来维持 Pi 的价格
- **精英收益**：奖励建立和维持网络的贡献

Pi - 令牌供应

令牌排放政策

1. 总最大供应量 = $M + R + D$.
1. M = 总采矿奖励
1. R = 总推荐奖励
1. D = 总开发者奖励

1. $M = \int f(P) dx$ 其中 f 是对数下降函数
1. P = 人口编号 (例如, 第一人加入, 第二人加入等)

1. $R = r * M$.
1. r = 推荐率 (推荐人和裁判员总数的 50% 或 25%)

1. $D = t * (M + R)$
1. t = 开发商奖励率 (25%)

M - 采矿供应 (基于每人铸造的固定采矿供应量)

与为全球人口创造固定硬币供应量的比特币相比，Pi 为每个加入网络的人创造了固定的 Pi 供应量，直至前 1 亿参与者。换句话说，对于加入 Pi 网络的每个人，预先固定量的 Pi。然后根据其参与程度和对网络安全的贡献，在该成员的生命周期内释放该供应。在成员的生命周期内，使用类似于比特币的指数递减函数释放供应。

R - 推荐供应（基于每人固定推荐奖励和共享黑白推荐人和裁判）

为了使货币具有价值，必须广泛分配。为了激励这个目标，该协议还生成固定数量的 Pi，作为推荐人和裁判（或父母和后代）的推荐奖金。这个共享池可以由双方在其生命周期内开采 - 当两者都是各方都在积极挖掘。推荐人和裁判都能够利用这个游泳池，以避免引用者能够“掠夺”他们的裁判的剥削模型。推荐奖金作为网络层面的激励来发展 Pi 网络，同时也激励成员之间积极保护网络。

D - 开发者奖励供应（附加 Pi 支持持续开发）

Pi 将通过“开发者奖励”为其正在进行的开发提供资金，该奖励与每个用于采矿和转介的硬币一起铸造。传统上，加密货币协议已经铸造了固定数量的供应，并立即进入库房。由于 Pi 的总供应量取决于网络中的成员数量，因此当网络扩展时，Pi 会逐渐减少其开发者奖励。Pi 的开发者奖励的渐进式创作旨在使 Pi 的贡献者的激励与网络的整体健康状况保持一致。

f 是对数递减函数 - 早期成员赚得更多

虽然 Pi 试图避免极度集中的财富，但该网络还寻求以相对较大的 Pi 份额奖励早期成员及其贡献。当像 Pi 这样的网络处于早期阶段时，

它们倾向于为参与者提供较低的效用。例如，假设拥有世界上第一部电话。这将是一项伟大的技术创新，但并不是非常有用。然而，随着越来越多的人获得电话，每个电话持有者从网络中获得更多的实用性。为了奖励提早来到网络的人，Pi 的个人挖掘奖励和推荐奖励随着网络中人数的增加而减少。换句话说，为 Pi 网络中的每个“时隙”保留一定量的 Pi。

效用：在线汇集和货币化我们的时间

今天，每个人都坐在一个名副其实的未开发资源宝库上。我们每个人都花几个小时在手机上。在我们的手机上，我们的每个观点，帖子或点击都为大公司创造了非凡的利润。在 Pi，我们相信人们有权利用他们的资源创造价值。

我们都知道，我们可以比单独做更多的事情。在今天的网络上，谷歌，亚马逊，Facebook 等大公司对个人消费者有巨大的影响力。因此，他们能够捕获个人消费者在网络上创造的价值的大多数。Pi 通过允许其成员汇集他们的集体资源来平衡竞争环境，以便他们可以分享他们创造的价值。

下图是 Pi Stack，我们看到了帮助我们的会员获取价值的特别有希望的机会。下面，我们将更详细地介绍这些领域。

介绍 Pi 堆栈 - 释放未充分利用的资源

Pi Ledger 和共享信任图 - 跨网络扩展信任

互联网上最大的挑战之一就是知道应该信任谁。今天，我们依靠亚马逊，eBay，Yelp 等提供商的评级系统来了解我们可以在互联网上进行交易的人。尽管我们，客户，在评估和审查我们的同行方面做了很多努力，但这些互联网中介机构捕获了创造这项工作的价值的狮子分享。

如上所述，Pi 的一致性算法创建了一个本地信任层，可以在没有中介的情况下扩展 Web 上的信任。虽然只有一个人的安全圈的价值很小，但我们各个安全圈的总体构建了一个全球“信任图”，帮助人们了解 Pi 网络上的谁可以信任。Pi Network 的全球信任图将促进陌生人之间的交易，否则这是不可能的。反过来，Pi 的本地货币允许每个为网络安全做出贡献的人捕获他们帮助创造的价值份额。

Pi 的注意力市场 - 保持未使用的注意力和时间

Pi 允许其成员汇集他们的集体注意力，创造一个比任何个人的注意力都更有价值的关注市场。构建在该层上的第一个应用程序将是当前托管在应用程序主屏幕上的*稀缺社交媒体渠道*。你可以想到*稀缺的社交媒体渠道*作为 Instagram 一次发布一个全球帖子。先锋可以通过分享内容（例如，文本，图像，视频）或提出寻求利用社区集体智慧的问题来打赌 Pi 吸引网络其他成员的注意力。在 Pi 网络上，每个人都有机会成为影响者或利用人群的智慧。到目前为止，Pi 的核心团队一直在使用这个频道来评估社区对 Pi 设计选择的看法（例如，社区对

Pi 徽标的设计和颜色进行了投票。)我们收到了许多有价值的回复和社区反馈意见。项目。一个可能的未来方向是打开任何先锋的关注市场，使用 Pi 发布他们的内容，同时扩大 Pi 网络上托管的频道数量。除了与同行交换关注之外，Pioneers 还可以选择与寻求他们关注的公司进行易货交易。美国人平均每天看到 4,000 到 10,000 个广告。公司争取我们的注意力并为此付出巨额资金。但是，我们客户不会从这些交易中获得任何价值。在 Pi 的注意力市场中，寻求接触 Pioneers 的公司将不得不在 Pi 中补偿他们的观众。Pi 的广告市场将严格选择加入，并为先锋们提供一个机会，让他们将最大的未开发资源之一货币化：他们的关注。

Pi 的易货市场 - 构建您的个人虚拟店面

除了为 Pi 网络提供信任和关注外，我们还希望 Pioneers 能够在未来贡献自己独特的技能和服务。Pi 的移动应用程序也将作为销售点，Pi 的成员可以通过“虚拟店面”向 Pi 网络的其他成员提供未开发的商品和服务。例如，一名成员在他们的公寓中提供未充分利用的房间，以便租给 Pi 网络上的其他成员。除了真实资产，Pi Network 的成员还可以通过他们的虚拟店面提供技能和服务。例如，Pi Network 的成员可以在 Pi 市场上提供他们的编程或设计技能。加班，Pi 的价值将得到越来越多的商品和服务的支持。

Pi 的分散应用商店 - 降低创作者的进入壁垒

Pi Network 的共享货币，信任图和市场将成为更广泛的分散应用生态系统的土壤。今天，任何想要启动应用程序的人都需要从头开始引

导其技术基础架构和社区。Pi 的分散式应用程序商店将允许 Dapp 开发人员利用 Pi 的现有基础架构以及社区和用户的共享资源。企业家和开发人员可以通过访问网络共享资源的请求向社区提出新的 Dapps。Pi 还将建立具有一定程度互操作性的 Dapps，以便 Dapps 能够在其他分散的应用程序中引用数据，资产和流程。

治理 - 人民的加密货币

第一代治理模型面临的挑战

信任是任何成功的货币体系的基础。产生信任的最重要因素之一是治理，或者随着时间的推移对协议实施变更的过程。尽管其重要性，但治理通常是加密经济系统中容易被忽视的方面之一。

比特币等第一代网络在很大程度上避免了正式（或“链上”）治理机制，有利于角色和激励设计相结合的非正式（或“脱链”）机制。从大多数衡量标准来看，比特币的治理机制非常成功，从一开始就允许协议在规模和价值方面大幅增长。但是，也存在一些挑战。比特币的经济集中导致了政治权力的集中。结果是，每个人都可能陷入大规模比特币持有者之间的破坏性战斗中。这一挑战的最新例子之一是比特币与比特币现金之间的持续战斗。这些内战可以在区块链的地方或地方结束。对于代币持有人来说，硬叉是通货膨胀的，可能会威胁到他们持有的股票的价值。

Pi 的治理模式 - 两阶段计划

在一篇[挑战链式治理优点的文章](#)中，以太坊核心开发人员之一 Vlad Zamfir 认为区块链治理 “不是一个抽象的设计问题。这是一个应用的社会问题。” 弗拉德的一个关键点是，“先验地”或在特定政治制度产生的特定挑战进行观察之前设计治理系统非常困难。一个历史的例子是美国的建立。在为期八年的实验之后，美国第一次民主实验“联邦条款”失败了。然后，美国的开国元勋们能够借鉴联邦条款的教训来制定宪法 - 一个更成功的实验。

为了建立一个持久的治理模式，Pi 将采取两阶段计划。

临时治理模型 (<5M 成员)

在网络达到临界质量的 500 万成员之前，Pi 将在临时治理模式下运作。该模型最类似于比特币和以太坊等协议目前采用的“离线”治理模型，Pi 的核心团队在指导协议的开发中发挥着重要作用。但是，Pi 的核心团队仍将严重依赖社区的投入。Pi 移动应用程序本身就是 Pi 的核心团队一直在征求社区意见并与 Pioneers 合作。Pi 接受社区批评和建议，这是通过 Pi 的登陆页面，常见问题解答和白皮书的开放评论功能实现的。每当人们在 Pi 的网站上浏览这些资料时，他们就可以在那里提交有关特定部分的评论，以提出问题并提出建议。

此外，Pi 的核心团队将开发更正式的治理机制。一个潜在的治理体系是流动民主。在流动民主中，每个先锋都有能力直接对某个问题进行投票，或者将他们的投票委托给另一个网络成员。流动民主将允许 Pi 的社区广泛而有效的成员资格。

Pi 的“制宪会议”（> 500 万会员）

在达到 5M 成员后，将根据之前对 Pi 网络的贡献成立临时委员会。该委员会将负责向更广泛的社区征求和提出建议。它还将组织一系列在线和离线对话，Pi 的成员将能够权衡 Pi 的长期构成。鉴于 Pi 的全球用户群，Pi Network 将在世界各地的多个地点开展这些会议，以确保可访问性。除了主持现场会议之外，Pi 还将使用其移动应用程序作为平台，允许 Pi 的成员远程参与该过程。无论是面对面还是在线，Pi 的社区成员都有能力参与制定 Pi 的长期治理结构。

路线图/部署计划

第 1 阶段 - 设计，分发，信任图引导程序。

Pi 服务器作为一个模拟分散系统行为的水龙头运行，因为它将在其生存时起作用。在此阶段期间，与主网络的稳定阶段相比，用户体验和行为的改进是可能的并且相对容易实现。所有用户铸造的硬币一旦启动，将被迁移到实时网络。换句话说，livenet 将在其生成块中预先填写第 1 阶段期间生成的所有帐户持有者余额，并继续像当前系统一样运行但完全分散。在此阶段，Pi 未在交易所上市，因此无法用任何其他货币“买入”Pi。

第 2 阶段 - Testnet

在我们启动主网之前，Node 软件将部署在测试网上。测试网将使用与主网相同的完全信任图，但使用测试 Pi 硬币。Pi 核心团队将在测试网上托管多个节点，但会鼓励更多先锋在 testnet 上启动自己的节

点。实际上，为了让任何节点加入主网，建议他们在 testnet 上开始。测试网将在第一阶段与 Pi 仿真器并行运行，并定期（例如每天）对两个系统的结果进行比较，以捕获测试网的间隙和缺失，这将允许 Pi 开发人员提出并实施修复。在完全同时运行两个系统之后，testnet 将达到其结果始终与仿真器匹配的状态。当社区感到准备好的时候，

第 3 阶段 - 主网

当社区认为该软件已准备好投入生产并且已在 testnet 上进行了全面测试时，将启动 Pi 网络的官方主网。一个重要的细节是，在向主网的过渡中，只有被证实属于不同真实个人的账户才会受到尊重。在此之后，第 1 阶段的水龙头和 Pi 网络仿真器将被关闭，系统将永远自行继续。该协议的更新将由 Pi 开发者社区和 Pi 的核心团队提供，并将由委员会提出。它们的实现和部署将取决于节点更新挖掘软件，就像任何其他区块链一样。没有中央机构将控制货币，它将完全分散。假用户或重复用户的余额将被丢弃。

如有疑问可加小助手