MeshX LABS

白皮书

imeshx.io

https://t.me/MeshXOfficialChinese

iMeshX888

2018

MeshX

Linking is mining

链 接 即 挖 矿

申明：本白皮书主要讲述了缦星生态公链的计算和运营逻辑，在主网上线之前，项目方保留对白皮书进行公开并开源修改的权利和解释权，同时，主网上线前的社群激励和前期商业逻辑将一并遵循主链逻辑，并做适度参数优化。

Linking is mining

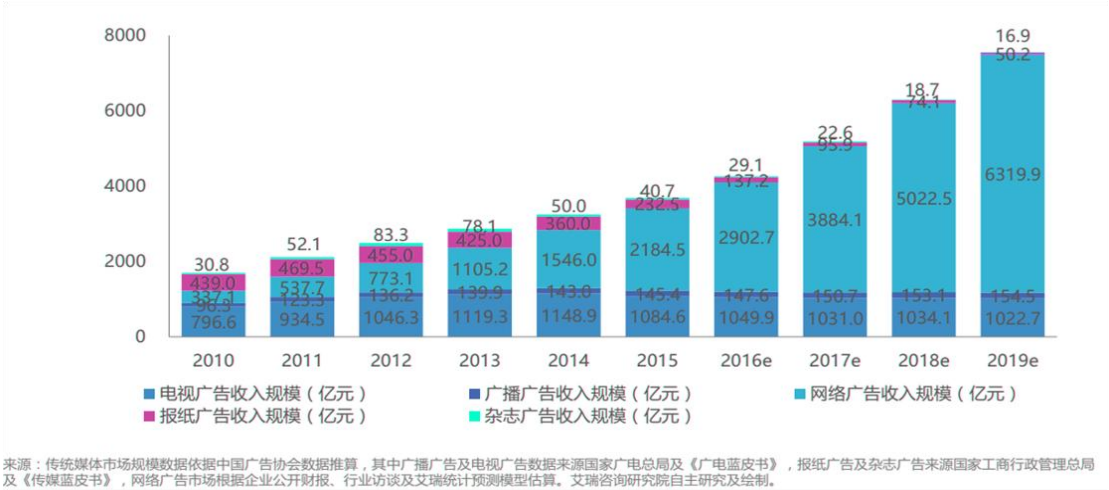
链 接 即 挖 矿

目录

1. 商业现状

1.1. 广告市场结构变化

目前纵观整个广告市场，尤其是发达国家，广告市场发展势头放缓，根据CTR的数据显示，2017年上半年中国广告市场整体增长0.4%，相较于去年同期 0.1%几乎持平，这表明整个市场的总体规模相对而言已经趋于恒定。但在整体市场趋于恒定的背后，是网络广告市场规模的增长与传统媒体广告市场的萎缩。



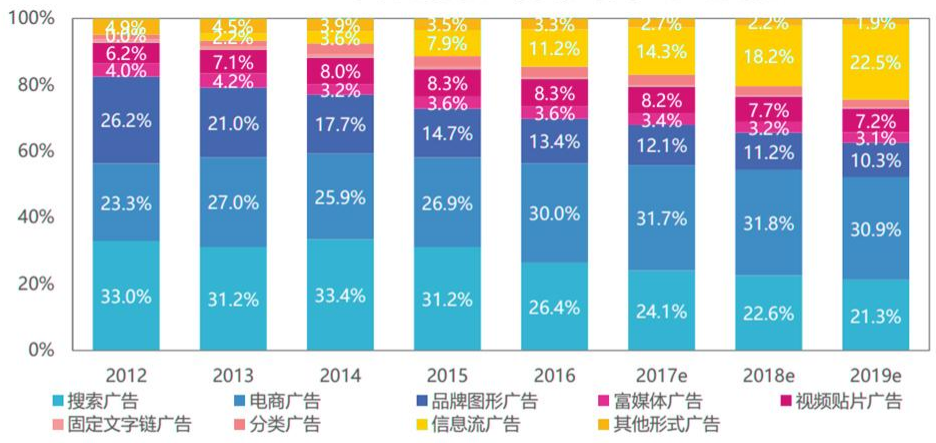
来源：传统媒体市场规模数据依据中国广告协会数据推算，其中广播广告及电视广告数据来源国家广电总局及《广电蓝皮书》，报纸广告及杂志广告来源国家工商行政管理总局及《传媒蓝皮书》，网络广告市场根据企业公开财报、行业访谈及艾瑞统计预测模型估算。艾瑞咨询研究院自主研究及绘制。

图 1.1 2010-2019 年中国五大媒体广告收入规模及预测

艾瑞咨询 2016 年度中国网络广告核心数据显示，中国网络广告市场规模达到 2902.7 亿元，同比增长 32.9%，未来增速仍会保持高位。网络广告市场中，主要有搜索广告、电商广告、品牌图形广告、富媒体广告、视频贴片广告、分类

广告、信息流广告等。与 MeshX 提供的广告形式相类似的有品牌图形广告和信息流广告。品牌图形广告市场规模于 2016 年达到 389.0 亿元，同比增长 21.0%。

随着程序化购买产业链的快速发展，广告主在品效合一方面的需求越来越高，作为最成熟的网络广告形式，品牌图形广告未来还将有较多资源投入到程序化购买的资源池，依然会有较多广告主重视该部分广告的投放，整体品牌图形广告市场将保持平稳发展。此外，2016 年的网络广告市场中，广告形式的创新与大数据应用及分析能力的提升成为主要特征。广告主对于曝光与效果的双重需求不断凸显，效果广告得到了更大的发展，信息流广告在 2016 年市场份额达到 11.2%，处于快速发展阶段。



注释：1.搜索广告包括搜索关键字广告及联盟广告；2.电商广告包括垂直搜索类广告以及展示类广告，例如淘宝、去哪儿及导购类网站；3.分类广告从2014年开始核算，仅包括58同城、赶集网等分类网站的广告营收，不包含搜房等垂直网站的分类广告营收；4.信息流广告从2016年开始独立核算，主要包括社交、新闻资讯、视频网站中的信息流效果广告等；其他形式广告包括导航广告、电子邮件广告等。
来源：根据企业公开财报、行业访谈及艾瑞统计预测模型估算。

图 1.2　2012-2019 年中国不同形式网络广告市场份额及预测

但品牌图形广告与信息流广告作为传统网络广告模式，有着不透明、可信度受质疑、投放效果难以评测、投放预算难以把控调节、投放体系依赖于其他 CDN 支持等缺点。对此需要高效优质的解决方案。

1.2. 消费者市场的 Wi-Fi 高需求

艾瑞数据显示，用户对于公共场所 Wi-Fi 需求重，近半用户在公共场所首选接入商业 Wi-Fi；具体使用情况为，超过两成用户每天都会使用商业 Wi-Fi，约八成用户平均每次使用时长超过 30 分钟；六成以上用户未来使用商业 Wi-Fi 的时长增加。调查显示，用户的 Wi-Fi 接入原因主要有：连接容易、网速较快以及网络稳定；接入目的主要有：游戏、视频、音乐、社交、下载等。

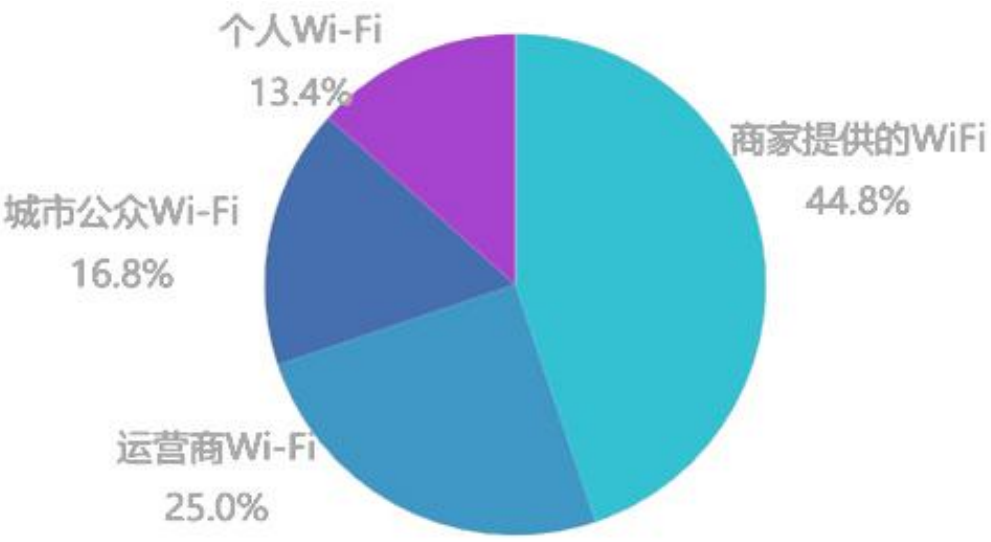


图 1.3 用户首选连接的公共场所 Wi-Fi 类型

此外，移动广告的高速发展也会推动 Wi-Fi 广告的发展，进一步保证广告流量贡献。2016 年，中国移动广告市场规模为 1750.2 亿，占比 60%，预计到 2019 年将接近 5000 亿，随着用户使用习惯的转移，未来几年移动广告在整体网络广告中的占比将持续增大，预计 2019 年该占比将接近 80%。

2. MeshX 的价值

2.1. 传统 WiFi 产品的缺陷

目前市场上主要的 WiFi 有五种：个人 WiFi、家庭 WiFi、城市公众 WiFi、通信运营商 WiFi、商业 WiFi。这五种类别的产品各有其劣势，如下表所示。

表 2.1 主要 WiFi 产品类别及劣势

WiFi 产品类别	劣势
个人 WiFi	只能在连接有线网的电脑附近使用，外出时使用不方便
家庭 WiFi	需要购买路由器，成本较高；只能在路由器覆盖的小范围内使用
城市公众 WiFi	需要政府投资布置，耗资巨大
通信运营商 WiFi	WiFi 用户需要付费使用该服务，成本较高
商业 WiFi	安装商业 WiFi 费用较高，导致广告宣传成本高，小商户无法负担

将市场现有的商业 WiFi 进行细分，各细分领域也存在着一定问题。

表 2.2 主要商业 WiFi 产品类别及劣势

WiFi 形式	连接方式	不足
商用服务平台	密码验证，网页跳转	安装成本高，小商户无法负担，普及度不高
WiFi APP	APP	WiFi 用户不信任这类 APP，担心个人信息被泄露
WiFi 平台	扫码登录	用户需要扫描商家二维码连接 WiFi，使用范围有限

2.2. MeshX 矿机网关技术特征

MeshX 是全球互联网无线覆盖生态平台，它拥有全球排名前三的网关制造能力，它的网关产品技术特征如下：

MeshX 即将发布一款共享无线加密网关，在这款网关组成的网络上可以应用区块链技术，构建 MeshX 链。MeshX 链的技术特征如下：

1）对于 MeshX 持有者来说，MeshX 区块链采用贡献率证明（POC）的共识算法来激励节点参与贡献率计算，其获取的 token 数与其贡献度成正比，并由共识机制根据其贡献度来分配。同时，提供代币（Token）激励用户参与、贡献资源。

2）对于广告主来说，投放路径和消耗全部记录在区块链上，彻底杜绝欺诈。

3）对于 WiFi 使用者来说，MeshX 采用软硬件结合双重加密（例如零知识证明算法），保护用户隐私。

2.3. MeshX 产品价值

MeshX 产品很大程度上解决了传统 WiFi 产品的痛点，并提供了一种基于 MeshX 链的新型广告投放模式。用户对优质 WiFi 的高需求为 MeshX 奠定了优良的受众基础，也为通过 MeshX 链投放的广告提供了流量保证。

基于 MeshX 产品可以构建生态链，生态链参与者（MeshX 矿机网关贡献者，广告发布者和 WiFi 使用者）可以从生态的发展中获益。

网关矿机贡献者可以根据 POC（Proof of Contribution）算法获得相应收益（Token）。广告投放者可定向投放广告到各 WiFi 终端，提高广告投放效率，广告投放费用只能使用代币（Token）支付。WiFi 使用者可以享受全球免费网络。数字资产（Token）在 Mesh 生态链中循环流动，生态链得以健康发展。

表 2.3 MeshX 的用户

Mesh WiFi 用户	Mesh WiFi 提供者	Mesh 广告商
可以免费随时随地使用 WiFi，并且个人信息得到保护，没有被不法商家泄露的风险	可以得到可观的广告费，避免 WiFi 设备闲置	用户主动阅读广告，投放效果可视化；区块链记录投放路径和消耗，杜绝欺诈

3. MeshX 链系统

3.1. 设计思想

■数据一致性

数据一致性其实是数据库系统中的概念，可以简单的把一致性理解为正确性或者完整性。而在分布式系统中，数据一致性往往指的是由于数据的复制，不同数据节点中的数据内容是否完整并且相同。

■可迁移机制

MeshX 节点会随着用户的流动增加、转移和退出。系统要保证增加 MeshX 节点时，能够扩充系统的边界、正常的运行，并且能够在一个记账周期内根据 MeshX 节点的贡献，分配相应的权益。同理，当 MeshX 节点从系统中移除时，不影响信息的传播、记账等功能，从而保证系统可伸缩。

■轻客户端

为了减轻 MeshX 节点的工作强度，MeshX 节点分为两类，包括轻节点和重节点。轻节点只向 MeshX 链提供资源，或使用 MeshX 链的资源。重节点将统计 MeshX 链中所有节点的贡献度、发放代币、记录交易信息。

■滞后结算策略

分布式交易体系的问题在于收款人很难校验之前的某位资产拥有者是否进行了双重支付（双花）。通常的解决方案是引入可信的第三方，如银行，来对每一笔交易进行检验，以防止双重支付。而如果想要排除第三方中介机构，那么交易信息就应当被公开，需要整个系统内的所有参与者，都有唯一公认的历史交易序列。因此，采用滞后结算交易的方式，通过记账节点对账来排除双重交易，保

证交易在交易期间内是首次出现的。

■权益锁定

为消除记账节点迁移、撤出 MeshX 系统带来的负面影响，维护系统的可靠运行，当记账节点获取到相应的权益后，会对其权益进行锁定，在一定时间内，这些权益不能进行交易。待记账节点的服务达到一定时间后，不再影响 MeshX 系统的正常运行，此时开始解除锁定。解除锁定后，用户可以自由交易权益。权益锁定期内，记账节点也能够获取相应的利息。

■快速达成共识

分布式交易体系的问题在于收款人很难校验之前的某位资产拥有者是否进行了双重支付（双花）。

■价值共识与激励

只要 MeshX 节点贡献自己的流量给生态链，那么 MeshX 节点就对生态链有贡献，那么它在 MeshX 中就有存在的价值。系统会根据其贡献程度，来分配相应的权益。并且 MeshX 节点在网络中存在的时间越长，它所获得的权益也就越多。

3.2. 系统概述

尽管区块链技术有一定的瑕疵(Eyal 2015, Eyal and Sirer 2013, Nayak et al. 2016)(AZURE 2016, CACHIN 2016, ROSS and SEWELL 2015)，但区块链技术(Garay, Kiayias, and Leonardos 2015, Nakamoto 2008)(2016)作为创造

信任的机器，具有分布式结构、建立信任、公开透明和时序不可篡改等技术优势，吸引了金融界和工业界的广泛关注，并开始被用于重塑交易系统，在降低交易成

本和提高交易效率方面效果显著。

基于工作量证明(Proof of Work, PoW)(Nakamoto 2008)是当今去中心化加密算法中最稳健的共识机制。PoW 主要用于选取一致的领导力节点，并给参与者合适的奖励。在区块链系统中，作为共识机制的参与者，矿工能够根据其算力被竞选为领导力节点。有了算力成本的约束，可以防止伪装成多节点的大算力攻击者，相应的代价就是要消耗大量的算力。算力消耗是基于工作量证明(Proof of Work, PoW)构建的区块链系统的问题所在，大量的系统计算资源和电能被耗费，使得系统的扩展性受到制约。

在 2011 年早期，权益证明 PoS(Proof of Stake)的概念被提出(Houy 2014)。直观的说，权益证明是拥有货币量证明的一种形式，币龄消耗是权益证明的一种形式。因此，权益证明被用在 PPcoin 中，并用来改进 PoW 工作机制耗费电能的缺点，且不容易被伪造。2014 年，以太坊设计了以太坊 PoS 架构，被称为友善小精灵 Casper(Casper the friendly ghost)(Houy 2014)，是一种 PoW 协议的 PoS 变种。在以太坊系统中，只有在验证人缴纳保证金的情况下，他的签名才有意义。客户端智能依赖于出自当前锁定保证金的验证人的块。已知当前锁定保证金的验证人，就可以鉴别出共识认可的链。不知道现在交纳保证金的验证人列表的客户端，必须先通过另外的信道获取这个列表，这个限制通过要求所有人用当前信息鉴别共识解决了“远程攻击”问题。

为了解决 PoW 挖矿效率低下、消耗资源的问题，MeshX 系统采用 PoW+PoTF(Proof of Traffic Flow)组合共识算法来构建，在工作量证明的过程中考虑系统用户的流量贡献值。

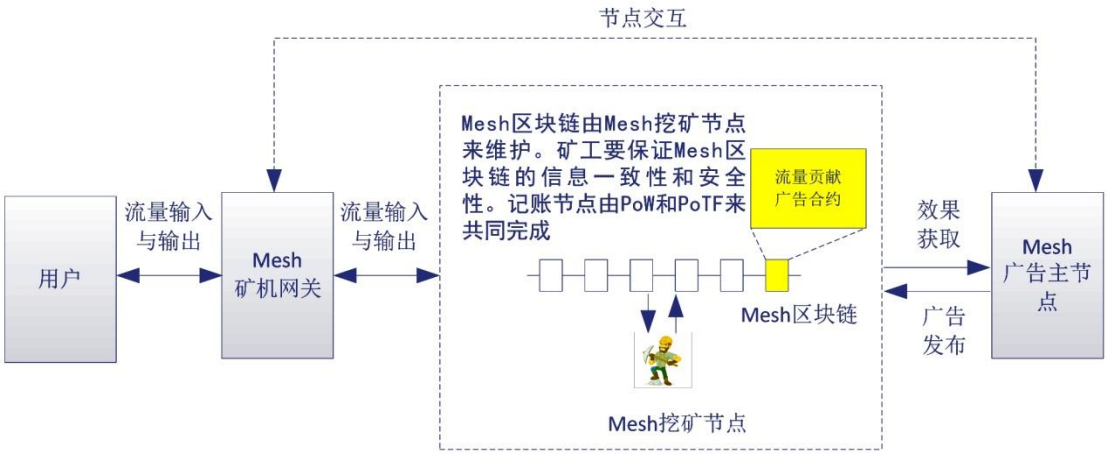


图 3.1 MeshX 系统结构概述

MeshX 链系统包括 MeshX 矿机网关节点、MeshX 链挖矿节点、智能使用终端和 MeshX 广告主节点组成。

■ MeshX 矿机网关节点：

矿机网关首先向 MeshX 系统提供流量贡献，然后产生加密随机数，并通过调用智能合约来传递有效流量贡献。在传递有效流量贡献的过程中，它会把有效流量贡献和随机数封装成一个区块，用自己的密钥加密后发送给 MeshX 链挖矿节点。

■ MeshX 链挖矿节点：

MeshX 链挖矿节点是有一定计算能力的服务器，是验证有效流量贡献的重要节点。挖矿节点收到矿机网关节点发送的有效流量贡献后，先进行验证，然后把信息打包到新的区块中，并广播到 P2P 网络之中。

■ MeshX 矿机网关使用终端：

终端连接到 MeshX 矿机网关后，产生有效流量，由矿机网关记录流量数据并广播到网络中去。

■ MeshX 广告主节点：

广告主节点可以在矿机网关中发布广告，根据广告覆盖的范围、持续时间等参数，支付费用。

3.3. MeshX 区块链

参考以太坊来设计 MeshX 链区块头（Wood, 2014），每个 MeshX 区块包含 MeshX 区块头和交易列表两部分，如下图所示。

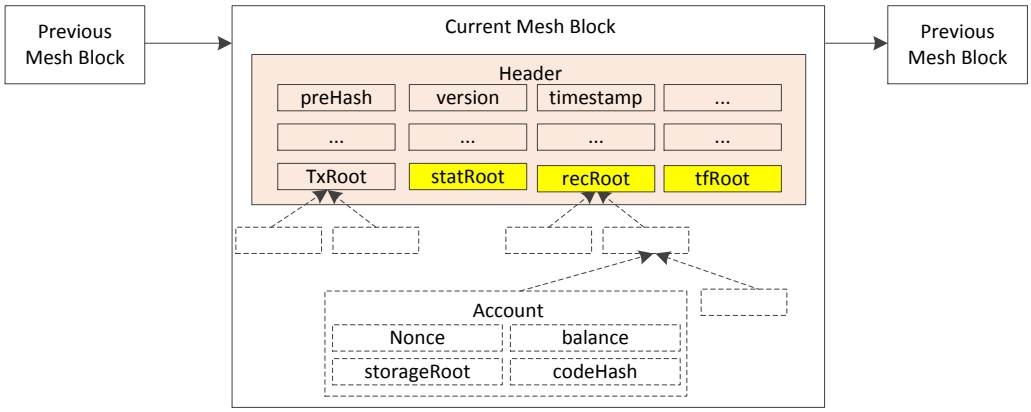


图 3.2 MeshX 区块结构

MeshX 区块头封装了父块 Hash、版本号、矿工地址、区块序号（高度）、Bloom 过滤器、当前代币量、代币使用量、难度级别、附加数据、混合摘要、随机数、交易根、状态根以及收据根等信息，其中交易根、状态根、收据根、流量根分别是交易树、状态树、收据树、流量树的根节点 Hash 值，而交易树、状态树、收据树、流量树是由 Merkle Patricia 树构造而成的。交易列表保存 MeshX 链交易信息。

基于 Merkle Patricia 树中存储所有信息的高效性，MeshX 链系统存在两种节点：全节点和轻节点。全节点同步下载整条 MeshX 链，从创世纪区块到当前区块，执行其中包含的所有交易。矿工（重节点）是全节点，会存储全部交易，因为他们在挖矿过程（记账过程）中需要校验或执行历史交易。无论如何，一个全节点包含了整个 MeshX 链重节点。轻节点仅仅下载 MeshX 链的头，从创世纪块到当前 MeshX 块的头，不执行任何的交易或检索任何相关联的状态。由于轻节点可以访问块的头，而头中包含了 3 个树的 Hash，所有轻节点依然可以很容易生成和接收关于交易、事件、余额等可验证信息的答案。

取得记账权的 MeshX 链节点将当前 MeshX 块链接到前一 MeshX 块，形成最新的区块主链。各个 MeshX 块依次链接起来，形成了一条从初始 MeshX 链到当前区块的最长主链，从而记录了 MeshX 链数据的完整历史，能够提供 MeshX 链数据的溯源和定位功能，任意数据（包括交易信息）都可以通过此链式结构顺藤摸瓜、追本溯源，这与比特币的链式结构相同(Nakamoto 2008)(Wood, 2014)。如图 MeshX 区块链式结构。

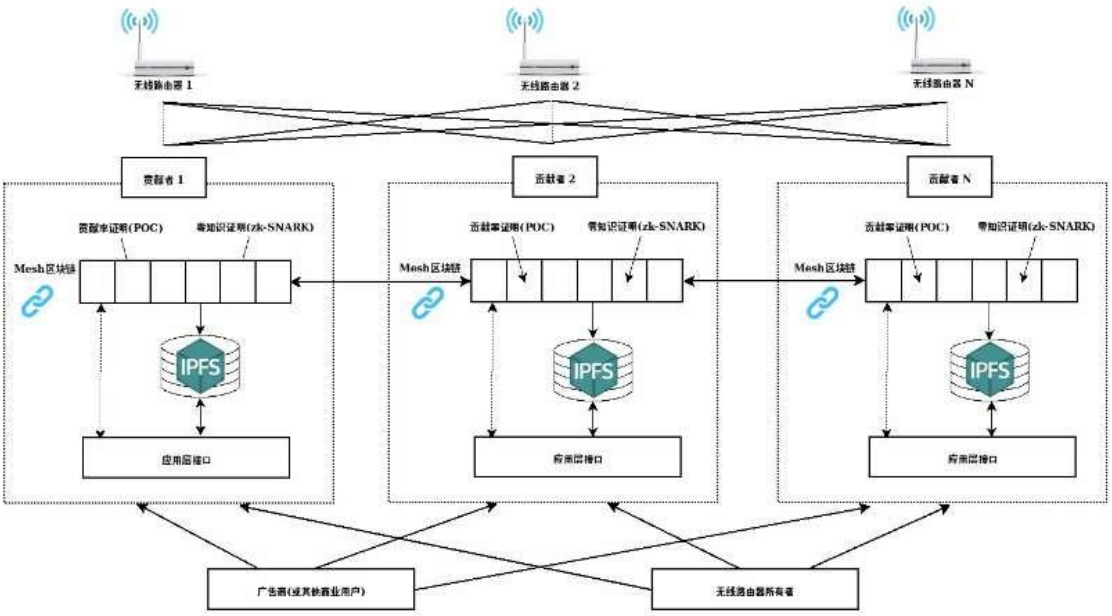


图 3.3 MeshX 块链式结构

如果短时间内有两个 MeshX 链节点同时算出两个新的 MeshX 块加以链接的话，MeshX 链主链可能会出现暂时的“分叉”现象，其解决方法是约定 MeshX 链节点总是选择累计流量最大的 MeshX 链。

3.4. MeshX 挖矿节点

为保证 MeshX 挖矿节点的权益，保证其能够公平的参与记账权的分配、公平参与区块的产生，同时为了让流量贡献值影响节点的挖矿能力，在工作量证明的同时，引入贡献参数。假设用 D(Difficult)表示当前挖矿难度，用 TFs(Traffic Flow)表示挖矿节点统计的流量。当且仅当当前挖矿节点的 TFs 高于 r%的系统中的其他挖矿节点，才有资格进行工作量证明，即：

$$MeshXProof(TFs,\ D,\ hash,\ r\%)$$

与 PoW 相同，当且仅当其解 hash 值的速度最快，将会获取创建新块、记账的权力。

4. 主要技术

4.1. 自组织组网

MeshX 链是区块链的外延，具有区块链所有的特性，如去中心化 、不可篡改、可信、安全、稳定、透明等。为了满足这些特性，MeshX 链系统节点应该具备分布式（分散化/去中心化）、自治性、开放可自由进出等特点。很明显，传统的基于中心服务器的网络拓扑结构或组网方式无法满足 MeshX 链系统的要求。比较而言，对等网络（Peer-to-peer network，P2P）（Qin 2002）（袁勇 and 王飞跃 2016）（如图 5.1） 具有分散化、可扩展性、健壮性、隐私性和高性能等特点（如表 5.1 所示）。

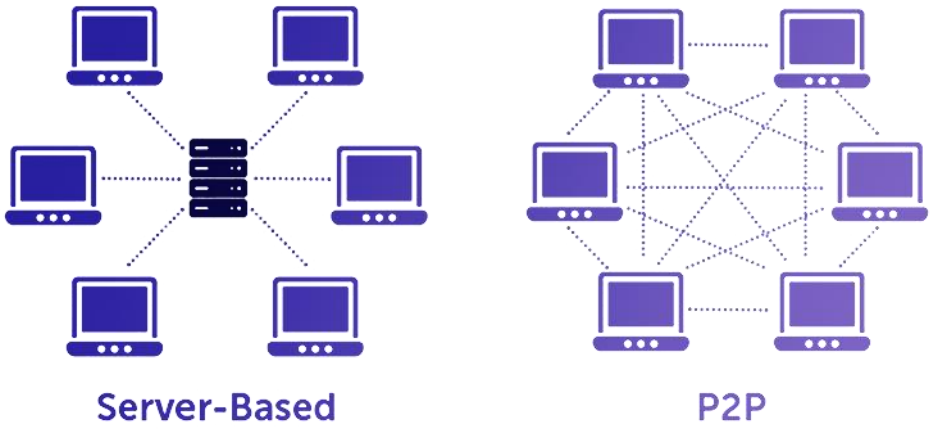


图 4.1 典型的网络拓扑结构

考虑由 k 个 MeshX 节点（Z1，Z2，… ， Zk）组成的 MeshX 链系统拓扑机构，如上图 4.1 所示。将上图网络中的 MeshX 链节点抽象为带权无向图 G=（V，E）。其中，V={ Z1，Z2，… Zi，…， Zk }为顶点集，顶点 Zi 表示 MeshX 链节点，k 为 MeshX 链节点的个数；E={eZ1，Z2,…，eZi，Zj,…，eZk-1，Zk}为边集，边 eZi，Zj 表示 MeshX 链节点 Zi 和 Zj 之间的通信链路。边上的权重 τZi，Zj 表示 MeshX 链节点{Zi， Zj}之间的通信时延。该无向图如图 4.2 所示。

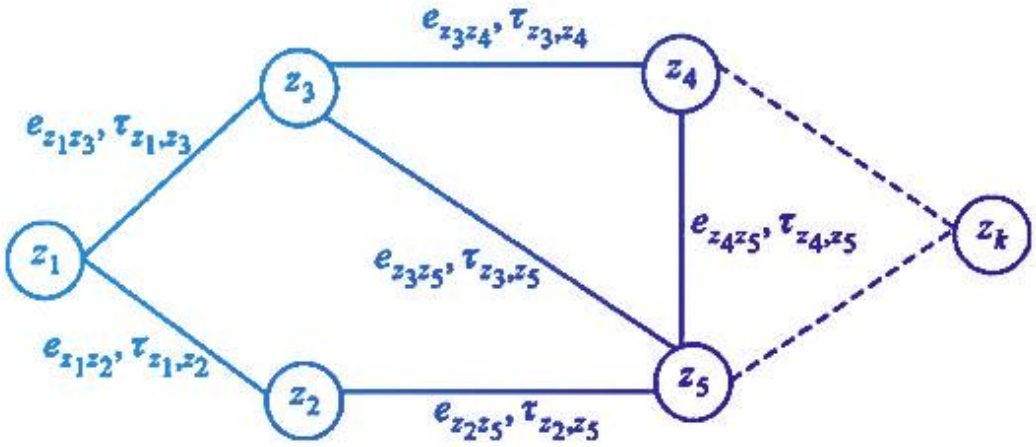


图 4.2 MeshX 链的节点之间消息传输示意图

图 4.2 每个 MeshX 链节点Z_i的计算能力假设为V_{z_i}。任务执行过程中，用户每次将计算存储任务D提交到其连接的 MeshX 链节点Z_i，Z_j将存储任务D划分为满足$d_i = \delta_i D$的若干子任务，并分配包括自己在内的计算节点进行计算。因此，整个计算存储任务D在边缘计算 MeshX 链网络中处理的总时间t可以表示为

$$t(\delta_i) = \max\left\{\frac{\delta_i D}{\upsilon_{z_i}} + \tau_{z_i,z_j} m_{z_i,z_j}\right\}$$

式中：$\delta_i D/\upsilon_{z_i}$表示 MeshX 链节点$Z_i$处理子任务$d_i$的时间；$\tau_{z_i,z_j} m_{z_i,z_j}$表示$\{Z_i, Z_j\}$之间的通信开销，其中$m_{z_i,z_j}$表示$\{Z_i, Z_j\}$之间是否存在子任务分配关系，$m_{z_i,z_j} = 1$表示存在子任务分配关系，$m_{z_i,z_j} = 0$表示不存在子任务分配关系。

由于分布式计算总任务的处理时间等于所有子任务中最大的计算延时，因此为了达到处理时延最小的目标，必须求一组最优的δ_i，使得目标函数t最小。综上所述，整个过程可以建模如下：

$$\min\left\{\max\left[\frac{\delta_i D}{\upsilon_{z_i}} + \tau_{z_i,z_j} m_{z_i,z_j}\right]\right\}, \quad i,j = 1,2,\cdots,k$$

$$\text{s.t.} \quad m_{z_i,z_j} = \begin{cases} 1, & \delta_i \neq 0 \\ 0, & \delta_i = 0 \end{cases}, \sum_{i=1}^{k} \delta_i = 1$$

因此每个 MeshX 链节点上应处理的子计算任务为$d_i = \delta_i D$，则k个 MeshX 链节点上分别处理的计算子任务可构成一个k维向量$d = [d_1, d_2, \cdots, d_k]^T$。考虑到具体情况，计算任务D可能来自任意一个节点，假设来自节点Z_1，由上述公式可知，在边缘计算 MeshX 链网络中处理计算任务D的总时间t可以表示为

$$t(d) = \max\left\{\frac{d_1}{\upsilon_{z_1}} + \tau_{z_1,z_1} m_{z_1,z_1}, \cdots, \frac{d_k}{\upsilon_{z_k}} + \tau_{z_1,z_k} m_{z_1,z_k}\right\}$$

因此，对 MeshX 链网络中每个计算节点上应处理的计算任务d_i的求解，即对任务向量d的求解，可归结为如下优化问题

$$d = \arg\min_{d\in 1}\{t(d)\}$$

$$s.t.\ d_i \geq 0, \sum_{i=1}^{k} d_i = D$$

上述优化问题的搜索空间 I为

$$I \triangleq \prod_{i=1}^{k}[D_{imin}, D_{imax}] = \prod_{i=1}^{k}[0, D]$$

对于上述优化问题的求解，目前有很多算法可以参考，例如带约束的粒子群优化负载均衡算法(Venter and Sobieszczanskisobieski 2002, Coello, Pulido, and Lechuga 2007)。

4.2. 流量贡献值证明算法

4.2.1. 节点类型

在 MeshX 链中，根据节点在网络中的作用，把节点分为轻节点和重节点。轻节点为 MeshX 链贡献流量。重节点则负责计算轻节点的流量贡献值、记录轻节点之间的交易行为，它是具有一定计算能力的云服务器。

4.2.2. 记账周期

流量贡献值记账周期是指 MeshX 链统计流量贡献值计算的周期。自 MeshX 链开始运行，每隔一个记账周期，将会选举一个或多个 MeshX 链重节点来统计轻节点的流量，用于分配 MeshX 的权益给轻节点。流量记账周期不宜设置过短，周期太短会使得系统中的节点频繁的统计流量，消耗大量的计算资源。流量记账

周期也不宜设置过长，过长的记账周期会降低贡献者的积极性，不利于 MeshX 链的建设。

交易记账周期是指对 MeshX 链中交易记账的周期。自 MeshX 链开始运行，每隔一个交易记账周期，将会选举一个或多个 MeshX 链节点来统计轻节点之间的交易数据，保证不会出现双重支付。相对流量记账周期，交易记账周期更短。过长的交易记账周期会使得系统中的交易不能够快速确认，不利 MeshX 币的流通。

4.2.3. 流量贡献值计算

■轻节点流量贡献值计算过程

轻节点贡献流量，然后把流量广播到网络中。重节点捕获轻节点广播的流量数据，根据轻节点贡献的流量情况计算出轻节点的流量贡献值，然后分配对等的权益。此外重节点要创建新区块，添加到区块链中。

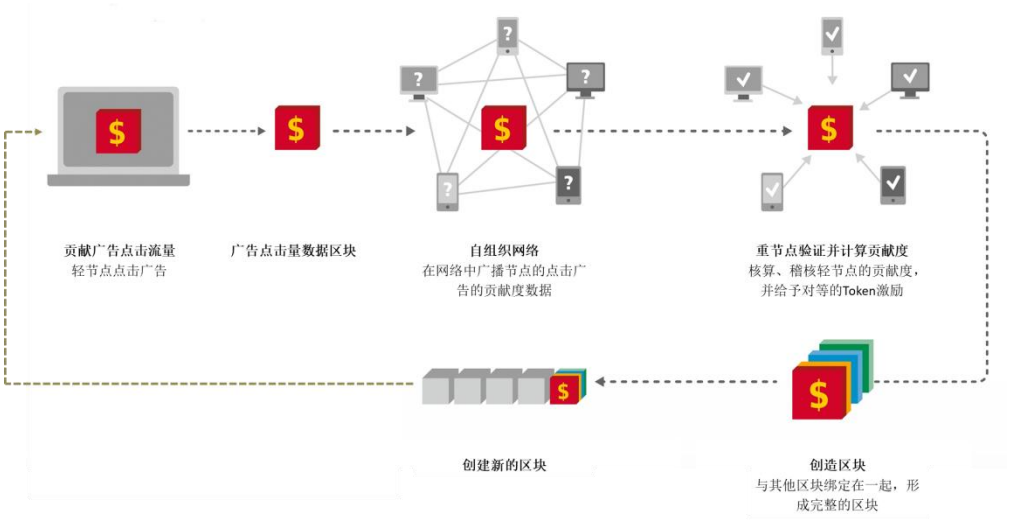


图 4.3 MeshX 链轻节点流量贡献值计算过程

轻节点流量贡献值计算

假设 1：轻节点贡献的流量是人为、主动和真实的行为，而非机器、被动和欺骗的流量行为。

假设 2：轻节点贡献的流量越多，其获取的边际效应越高。

在假设 1 和假设 2 成立的情况下，我们可以根据 MeshX 链节点在一个记账周期内的流量总和来计算 MeshX 链轻节点的贡献值。定义效用函数U( )，用来计算 MeshX 链轻节点在 T 时刻的贡献值：

$$works(T) = U(TFs)$$

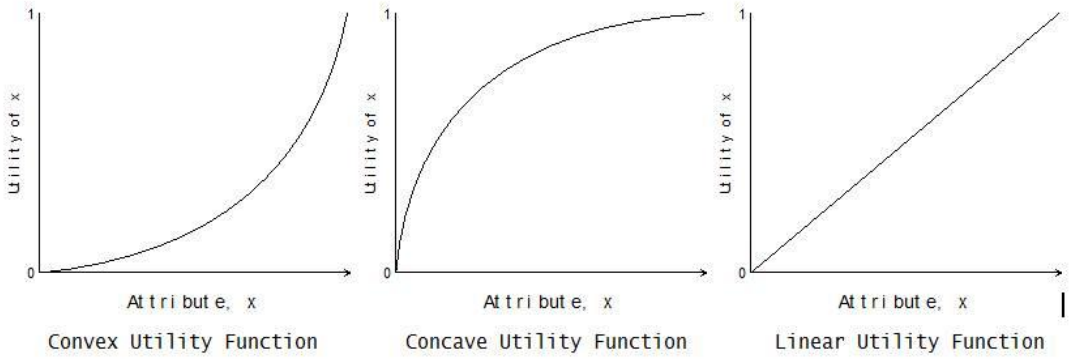


图 4.4 效用函数曲线

可选取凸函数、凹函数或者线性函数作为效用函数。若流量的贡献较为平均，可以选取线性效用函数。若系统中存在欺诈流量的行为，为了防止这些节点刷流量，可以采用凹函数作为效用函数，即随着流量的增加，这些节点因流量带来的收益降低至 0.

$$\frac{\Delta works(T)}{\Delta T} \to 0$$

为了鼓励节点长期、稳定的流量贡献，增加对 MeshX 链的黏性，引入贡献值年化利息 θ 的概念。轻节点留在 MeshX 链时间越长，其获得的收益越高。轻节点在 T 时刻的复利贡献量记为wworks(T)。设贡献值记账周期为Δt_c天，T 时刻 MeshX 链节点贡献量为works(T)，之前的贡献量为works(t)（$t = 1,2,\dots,T-1$），

年化利率为 θ，那么 T 时刻 MeshX 链节点的复利贡献量wworks(T)定义为：

$$\mathrm{wworks(T)} = \mathrm{works(T)} + \sum_{t=1}^{T-1} \mathrm{works(t)} \cdot (1 + \theta \cdot \frac{365}{\Delta t_c})$$

其中 $\theta \cdot \frac{365}{\Delta t_c}$是 MeshX 链轻节点持续为系统贡献流量获取的额外收益，相当于 MeshX 链轻节点的贡献值利息。

4.2.4. 重节点选举

MeshX 链中的重节点必须要有足够的流量才有资格被选举为重节点。假设记账周期产生的数据总量（Data Volumn）共计 X 千字节，若 MeshX 链节点的计算能力 ≤X 千字节，那么该 MeshX 链节点将不具有资格参选重节点。与 PoS 的思想相似，重节点代表一系列轻节点的权益，其代表的轻节点越多，被选择作为重节点的可能性越高。假设 T 时刻 MeshX 链节重节点 i 记录的复利流量的贡献总量为iTwworks(T)，那么它是否有资格记账由下面的公式来确定：

$$\text{记账权资格} = \begin{cases} 0, & \text{if } \mathrm{iTwworks(T)} \le s \\ 1, & \text{if } \mathrm{iTwworks(T)} > s \end{cases}$$

s是流量统计的阈值，用来确定记账资格，选出少数的具有记账能力的重节点。可以选取 20%的重节点来记账，并通过 PoW 挖矿机制来从 20 个重节点中选出重节点。

4.2.5. 流量共享的权益分配

被选举来记账的重节点将同步所有其他重节点的流量贡献值的总额，统计 T 时刻 MeshX 链上所有轻节点的总复利流量贡献的总量wworks(T)，它等于所有 MeshX 链节点的流量贡献量的和，即：

$$\mathrm{Twworks} = \sum_{i=1}^{n} \mathrm{iTwworks(T)}$$

其中iTwworks为第 i 个重节点记录的总贡献量，n 为总的重节点数。

假设 T 时刻所处的周期待分配的 MeshX 权益总量为 MeshX Token(T)，那么第 i 个轻节点根据其贡献的流量总和获得的 Token 权益数量为：

$$\text{MeshX Token}(T|i) = \frac{\text{wworks}(T|i)}{\text{Twworks}} \cdot \text{MeshX Token}(T)$$

在完成权益分配之后，重节点将把计算结果封装到流量贡献总额的记账区块中，并广播到网络中，待其他重节点验证后获得记账奖励。

4.2.6. 交易记账过程

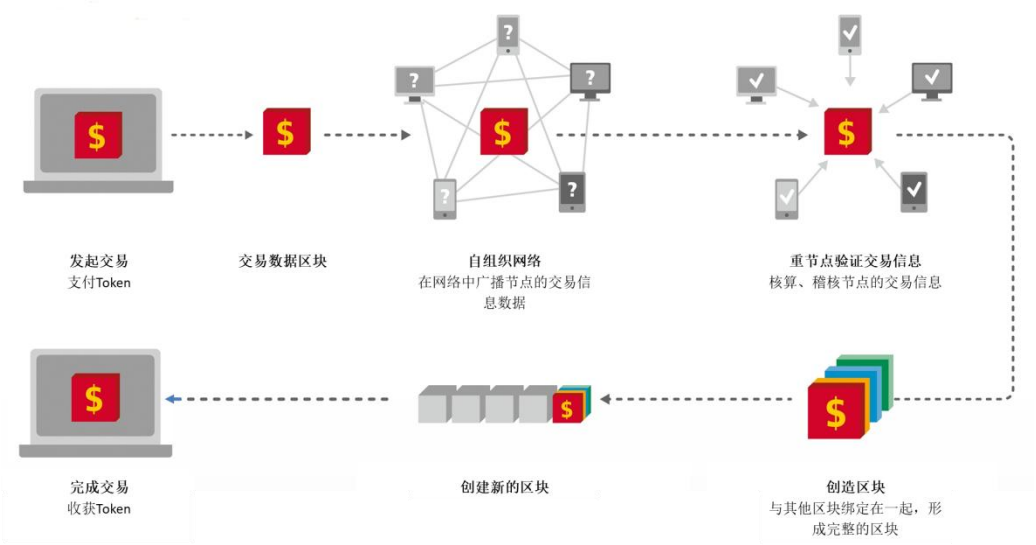


图 4.5 交易过程

交易是指 MeshX 链节点之间的资产转移行为。定义 UTXO（Unspent Transaction Outputs）是 MeshX 链节点未花费的交易输出。交易构成了一组链式结构，所有合法的 MeshX 链节点交易都可以追溯到前向一个或多个交易的输出，这些链条的源头都是挖矿奖励，末尾则是当前未花费的交易输出。

当节点发起交易，会把交易数据打包并广播到网络中。重节点捕获其他节点

的交易数据后，将核算、稽核节点交易信息，并创建区块。区块创建完成后，交易将被确认，并完成。为了防止重节点交易中的欺诈行为，它不能进行任何交易，也不能通过贡献来获取收益。它的收益主要来源于挖矿和交易手续费，挖矿指的是计算贡献量和确认交易有效性时创造新区块的过程。

4.3. 持有者场所识别

持有者在不同的场所贡献路由器资源带来的商业价值是不同的。场所主要包括公共场所、办公场所、家庭场所。各场所价值特点如下表所示：

表 4.1 MeshX 的安装场所

场所	价值特点
公共场所	□ 在线时长较短 □ 并联用户较多 □ 服务用户较多 □ 广告效益较高 □ 数字资产（Token）收益最高
办公场所	□ 并联用户多. □ 单用户在线时长较长 □ 在网时间相对固定 □ 广告触达用户少，但广告效果佳 □ 数字资产（Token）收益次之
家庭场所	□ 并联用户少 □ 邻里共享 □ 广告价值弱. □ 数字内容消费高频 □ 数字资产（Token）收益最弱

流量贡献值计算过程中需根据路由器所在的不同场所来调整最终贡献值计算。

4.4. 防止持有者恶意贡献行为

路由器的贡献值直接和持有者的收益挂钩，因此会有部分持有者恶意提高贡献值（如连接次数）以获取更多的收益。为了避免这种行为，需要在贡献值计算过程中对此行为施加惩罚，使得恶意持有者获得收益趋近于零。

5. 区块链经济模型

5.1. MeshX 币价值基础

MeshX 币是 MeshX 链上的原生资产，MeshX 币的价值起源是其能够方便的表征和度量 MeshX 链上的数字化经济活动。MeshX 币既代表 MeshX 链的所有权又代表使用权：使用 MeshX 链投放广告需用 MeshX 币支付一定的费用，体现 MeshX 币的使用权特性；持有 MeshX 币，代表拥有 MeshX 币的一部分，相当于 MeshX 链的股东，能够参与到 MeshX 链治理的最高决策，体现 MeshX 币的所有权特性。

5.2. 激励机制

MeshX 网络包含其内建的 MeshX 币，在网络内包含一种 MeshX 币的原因是多重的。首先，MeshX 币被奖励给矿工以促进网络安全；其次，MeshX 币被奖励给路由器持有者，激励持有者贡献资源，促进网络生长；最后，用它来支付交易费用是一种反欺诈机制。类似 Hashcash 的以交易为单位的工作量证明和放任自由是收取交易费的两个替代方案，前者浪费资源并且对于低档计算机和智能手机是一种不公平的折磨，后者将会导致网络立刻被无限循环的“逻辑炸弹”合约淹没。

此外还要设定惩罚规则规范持有者的贡献行为，避免恶意伪造贡献行为产生。

5.3. 发行机制

5.3.1. 发行模型

MeshX 系统按节点数量的变化分为上线期，成长期，稳定期。其中上线期通过创世区块发行量为 1.5M，然后每年增加供应量 pM，其中 p<1。那么理论 MeshX 币供应量为 S(t)=1.5M+pM*t=M(1.5+p*t)，又计为 S(t)=S(t-1)+ΔS,其中 ΔS=pM；MeshX 币增长率为 g(t)=(S(t+1)-S(t))/S(t)=p/(1.5+p*t)。

永久线性增长模型从长期来看“MeshX 供应增长率曲线”是趋于零的，如下图所示。

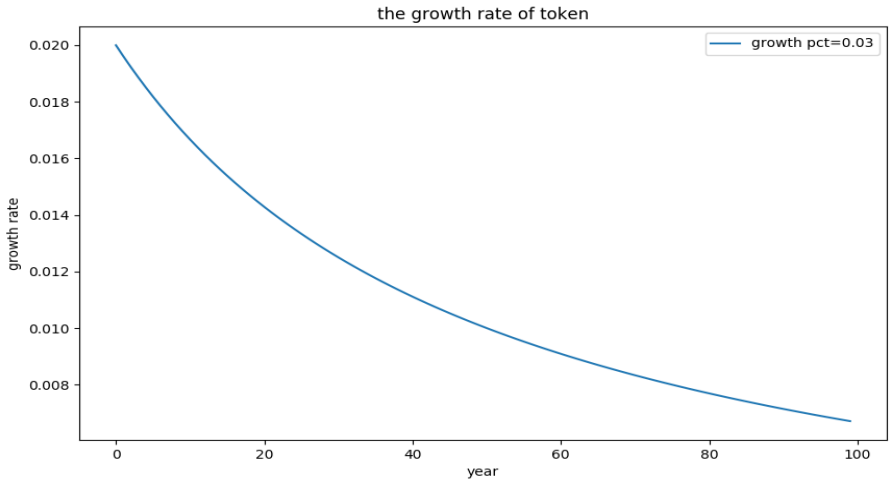


图 5.1 MeshX 供应增长率曲线

另外随着时间流逝总会发生因为粗心和死亡等原因带来的币的遗失，假设币的遗失是每年 MeshX 币供应量的一个固定比例，那么最终总的流通中的 MeshX 币供应量会稳定在一个等于年 MeshX 币发行量除以遗失率的值上。设每年 MeshX 币遗失率为 q(q<1)，那么各年度实际 MeshX 币供应量为：Sr(t)=(Sr(t-1)+ΔS)*(1-q)，流通总量趋近于 pM/q。

下表详细列出了各年度 MeshX 币供应量和遗失量。

表 5.1 MeshX 供应量和遗失量

年度	实际 MeshX 币供应量	理论 MeshX 币供应量	MeshX 币遗失量
0	1.5M	1.5M	0
1	Sr(1)=S(1)-S(1)*q	S(1)	S(1)*q
2	Sr(2)=S(2)-S(1)*q-(S(2)-S(1)*q)*q	S(2)-S(1)*q	(S(2)-S(1)*q)*q
t	Sr(t)=(Sr(t-1)+ΔS)*(1-q)	Sr(t-1)+ΔS	(Sr(t-1)+ΔS)*q

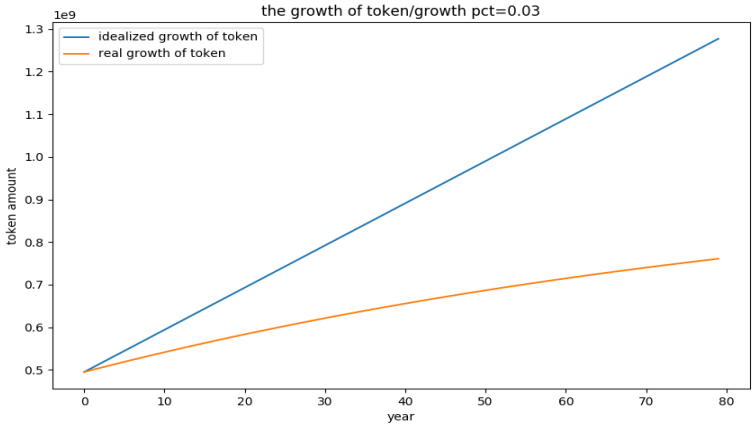


图 5.2 理想和实际的 MeshX 增长曲线

预定方案决定 MeshX 币供应总量不超过 1,000,000,000，那么为了确保 50 年内理论 MeshX 币供应量和 MeshX 系统的整个生命周期内实际 MeshX 币供应量不超过 1,000,000,000 ，算出 p=0.03，遗失率 q=0.01，$M^{\sim}$=330,000,000;当供应量达到 3M 时，每年有 0.03M 被挖出同时有 0.03M 丢失，达到一个均衡，如下图所示。

假设 MeshX 网中节点数量按 S 型曲线增长，如下图所示。

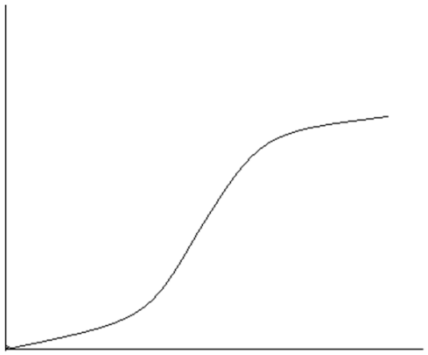


图 5.3 MeshX 节点增长速度

按照前面所述，每年新增 MeshX 币 10,000,000。随着节点数增加，周期内交易量增加，而单个区块容量有限，每个周期产生的区块总数相应增加。为了确保成长期内单个节点一定的贡献量所能获得的奖励数量大致稳定，设定第一年每日的 MeshX 币供应量模型如下文所示。

上线期后首日发行 MeshX 币 N，MeshX 历史区块数量增加 1 倍后，每日发行 MeshX 币数量增加一倍；设第一年内每日 MeshX 币发行数量的最大调整次数为 n。假设 N=10,000，为了使第一年发行的 MeshX 币数量不超过 10,000,000，可算得 n 最大为 3。从第二年开始，每日 MeshX 币发行数量固定为 27400。

5.3.2. MeshX 币单位

MeshX 币单位包括：MeshX，mMeshX，μMeshX；

它们的数量关系如下：

1 MeshX =1000 mMeshX =1000000 μMeshX

5.3.3. 挖矿难度

每个周期 MeshX 链系统自动设定一个流量贡献值阈值，流量贡献值超过阈值的节点获得记账授权。为了使每个周期获得记账授权的节点比例维持在一定水平上，系统将根据上个周期拥有记账授权的节点比例来调整当前周期的流量贡献值阈值。定义流量贡献值阈值为挖矿难度。

MeshX 的区块平均每 t 分钟生成一个。这就是 MeshX 的心跳，是 MeshX 发行速率和交易确认速度的基础。不仅是在短期内，而是在几十年内它都必须要保持恒定。在此期间，计算机性能将飞速提升。此外，参与挖矿的人和计算机也会不断变化。为了能让新区块的保持 t 分钟一个的产生速率，挖矿的难度必须根据这

些变化进行调整。事实上，难度是一个动态的参数，会定期调整以达到每 t 分钟一个新区块的目标。简单地说，难度被设定在，无论挖矿能力如何，新区块产生速率都保持在 t 分钟一个。

5.3.4. MeshX 币生成

每个周期内网络设备不断产生流量贡献值数据，并共识到各个节点的内存中，等到周期结束时记账节点开始计算各设备的流量贡献值，并根据流量贡献值给设备发放奖励。奖励以交易的形式被记账节点打包到新区块中。新区块创建后被记账节点广播到全网的区块链节点，进行流量贡献值证明校验，区块内交易校验；如果校验通过，区块链节点将在本地的区块链末尾添加新交易区块。

此外，MeshX 用户之间也会产生代币交易，这些交易由记账节点打包到区块中，并经全网共识添加到区块链中。记账节点获得挖矿奖励，奖励以交易的形式发放。

5.3.5. MeshX 币交易的生命周期

一笔 MeshX 币交易的生命周期起始于它被创建的那一刻，也就是诞生。 随后，MeshX 币交易会被一个或者多个签名加密，这些签名标志着对该交易指向的 MeshX 币资金的使用许可。接下来，MeshX 币交易被广播到 MeshX 币网络中。在 MeshX 币网络中，每一个 MeshX 节点（MeshX 币交易参与者）验证、并将交易在网络中进行广播，直到这笔交易被网络中大多数节点接收。最终，MeshX 币交易被一个记账节点验证，并被添加到区块链上一个记录着许多 MeshX 币交易的区块中。

一笔 MeshX 币交易一旦被记录到区块链上并被足够多的后续区块确认，便

成为 MeshX 币总账簿的一部分，并被所有 MeshX 币交易参与者认可为有效交易。于是，被这笔交易分配到一个新所有者名下的 MeshX 币资金可以在新的交易中被使用——这使得所有权链得以延伸且再次开启一个新的 MeshX 币交易生命周期。

5.4. 分配机制

MeshX Token(MSX)分配模型如下：

6. 参考资料

Aksu, Hidayet, Leonardo Babun, Mauro Conti, Gabriele Tolomei, and A. Selcuk Uluagac. 2018. "Advertising in the IoT Era: Vision and Challenges." IEEE Communications Magazine no. PP (99).

Chen, Lin, Lei Xu, Nolan Shah, Zhimin Gao, Yang Lu, and Weidong Shi. 2017. "On Security Analysis of Proof-of-Elapsed-Time (PoET)."

Coello, C. A. C., G. T. Pulido, and M. S. Lechuga. 2007. "Handling multiple objectives with particle swarm optimization." IEEE Transactions on Evolutionary Computation no. 8 (3):256-279.

Coker, George, Joshua Guttman, Peter Loscocco, Amy Herzog, Jonathan Millen, Brian O'Hanlon, John Ramsdell, Ariel Segall, Justin Sheehy, and Brian Sniffen. 2011. "Principles of remote attestation." International Journal of Information Security no. 10 (2):63-81.

Eyal, Ittay. 2015. "The Miner's Dilemma." ieee symposium on security and privacy:89-103.

Eyal, Ittay, and Emin Gun Sirer. 2013. "Majority is not Enough: Bitcoin Mining is Vulnerable." financial cryptography:436-454.

Garay, Juan A, Aggelos Kiayias, and Nikos Leonardos. 2015. The Bitcoin Backbone Protocol: Analysis and Applications *. Paper read at theory and application of cryptographic techniques.

Goldreich, Oded, and Hugo Krawczyk. 1990. "On the composition of zero-knowledge proof systems." Siam Journal on Computing no. 25 (1):268-282.

Goldreich, Oded, Silvio Micali, and Avi Wigderson. 1991. "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems." Journal of the Acm no. 38 (3):690-728.

Guilford, J. P. 2011. "Varieties of divergent production." Journal of Creative Behavior no. 18 (1):1-10.

Houy, Nicolas. 2014. "It Will Cost You Nothing to 'Kill' a Proof-of-Stake Crypto-Currency." Social Science Electronic Publishing no. 34 (2).

Miralles-Pechuán, Luis, Dafne Rosso, Fernando Jiménez, and Jose M. García. 2016. "A methodology based on Deep Learning for advert value calculation in CPM, CPC and CPA networks." Soft Computing no. 21 (3):1-15.

Nakamoto, Satoshi. 2008. "Bitcoin: A peer-to-peer electronic cash

system." Consulted.
Nayak, Kartik, Srijan Kumar, Andrew J Miller, and Elaine Shi. 2016. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack. Paper read at ieee symposium on security and privacy.
Qin, L. 2002. Search and Replication in Unstructured Peer-to-Peer Network. Paper read at ICS.

Roldán-García, María Del Mar, José García-Nieto, and José F. Aldana-Montes. 2017. "Enhancing Semantic Consistency in Anti-Fraud Rule-Based Expert Systems." Expert Systems with Applications no. 90.
Smyth, Ben, Mark D. Ryan, and Liqun Chen. 2015. "Formal analysis of

privacy in Direct Anonymous Attestation schemes ☆." Science of Computer Programming no. 111:300-317.
Venter, Gerhard, and Jaroslaw Sobieszczanskisobieski. 2002. "Particle Swarm Optimization." Aiaa Journal no. 41 (8):129-132.
Xing, Bin Cedric, Mark Shanahan, and Rebekah Leslie-Hurd. 2016. Intel®; Software Guard Extensions (Intel®; SGX) Software Support for Dynamic Memory Allocation inside an Enclave. Paper read at Hardware and Architectural Support for Security and Privacy.
袁勇, and 王飞跃. 2016. "区块链技术发展现状与展望." 自动化学报 no. 42 (4):481-494.
Azure, M. Blockchain as a service. https://azure.microsoft.com/en-us/solutions/blockchain/, 2016.
Wood G. Ethereum: a secure decentralised generalised transaction ledger, Ethereum Project Yellow Paper (2014) 1-32.
Cachin, C. Architecture of the Hyperledger blockchain fabric. In Workshop on Distributed Cryptocurrencies and Consensus Ledgers (2016).
Ross, R., AND Sewell, J. Foldingcoin white paper. https://web.archive.org/web/2016 1022232226/, http://foldingcoin.net/the-coin/white-paper/, 2015
Matchcraft 2016. https://www.matchcraft.com/how-google-facebook-are-dominating-online-mobile- advertising/
Emarketer 2015. https://www.emarketer.com/Article/Total-Media-Ad-Spending-Growth-Slows- Worldwide/1012981
Statista 2015. https://www.statista.com/topics/2464/yahoo/.