Mainframe：基于Web3的通信层

Adam Clarke, Austin Craig, Brad Hagen, Carl Youngblood, Clément Jaquier, Diogo Perillo, Luca Tavazzani, Matt Larson, Mick Hagen, Miloš Mošić, Paul Le Cam, Shane Howley, PhD

摘要

现有网络协议中存在的缺陷使网络安全难以得到保障。Mainframe是一个蕴含奖励机制的完全去中心化的通信层，它提供安全可靠的封包路由、数据包投递、数据包持有、文档储存和数据服务。Mainframe配备的安全模型不仅有加密技术，还能抵挡审查和监控。本白皮书详细描述了Mainframe平台运作、激励模型、代币经济和发展路线图。

关键词：协议；网络；通信；信息通讯；代币；经济学；安全；密码学；去中心化；区块链；智能合约

mainframe

基于Web3的通信技术层

mainframe.com

Contributors

Adam Clarke . Austin Craig . Brad Hagen . Carl Youngblood . Clément Jaquier . Diogo Perillo
Luca Tavazzani . Matt Larson . Mick Hagen . Miloš Mošić . Paul Le Cam . Shane Howley, PhD

本文档并非招股说明书，所提供信息仅供参考。

白皮书V1.0

Mainframe

通信势不可挡

自十九世纪中期首次公开面世以来，互联网推动了许多前所未有的创新创造，连接各式设备并支持新兴应用软件，这远远超出了发明者们对它的预期。如今全球超出一半人口，将近40亿人在使用互联网。

互联网取得巨大成功的同时也面临新的挑战。许多第三方传递用户信息，却往往不与用户的最大利益保持一致。政府监管和恶意代理也带来额外威胁。数十年前打造的整个互联网的基础架构，如今成为了各利益方的逐利工具。与有价信息打交道的人的隐私和福祉无法得到保障。仅在商界，近期新闻头条不是安全漏洞导致股价大跌、交易失败，就是公司机密被泄漏等。仅凭现有方法去弥补这些安全漏洞，已希望渺茫。

为更有效解决以上问题，新的工具应运而生。在Mainframe这样一个前所未有的通信平台上，客户能获得独一无二的安全解决方案，其中包括：

- **数据隐私性:** 完全端对端的群加密
- **监视抵抗性:** 节点关系可隐藏
- **审查抵抗性:** 隐藏节点关系，防止通信干扰

“美国宪法中未列入任何私人沟通的权利在那时没有人预料到这样的基本权利会在今天受到阻碍”

Whitfield Diffie
非对称加密算法联合发明人

Mainframe的通信基础架构完全去中心化，且无主机控制。代币经济可以激励网络性能，如：

- 奖励封包路由
- 奖励包储存以便之后检索
- 奖励文档储存
- 奖励数据服务

Mainframe提供前所未有的通信安全，又不牺牲服务的便捷性。

中心化系统侵犯隐私和自由

在比特币区块链的创世块上，创建者中本聪留下了这样一句话：

“2009年1月3日《泰晤士报》，财政大臣在实施第二轮银行紧急援助的边缘”。

对于这句话没有更多的解释或评述，但很多人认为它恰好是当天伦敦《泰晤士报》的新闻头条[1]有以下两个原因：一是，如此这般便将比特币的诞生同一个可证实的历史事件关联在一起；二是，它暗示了整个大氛围下的信任危机、滥用职权和制度失灵。

2008至2013年期间，全世界范围内人们对政府、企业和媒体的信任下滑有目共睹[2]。这六年中还发生了金融危机，政府救助和阿拉伯之春运动。在阿拉伯之春运动中，数百万民众通过Facebook或WhatsApp这样的网络平台向政府发声，表达强烈不满需求。政权颠覆间，成千上万的民众不幸丧生，多国陷入内战。早期的阿拉伯之春抗议活动引发占领华尔街运动，这场运动主要也是民众通过社交平台发起的，据2012年的一整年数据显示，该运动的参与者来自82个国家[3]、近1000座城市。2013年夏季，爱德华·斯诺登向美国民众和全世界曝光拉网式监视的惊人消息在所有虚拟平台和各种通信模式上广为传播。以上提及的这每一个事件都凸显出完全去中心化的通信是多么重要，它不依赖于第三方，用户信息能得到保护。在某些情况下，它甚至关乎生死。

在工作场所采用中心化的架构需消耗巨额成本。定期检修成本高昂且不便利，但同恶意威胁相比，这些实在不算什么 。《连线》[4]、《财富》[5]杂志、IBM[6]和其他媒体多次强调、反复提及“数据是新的推动力”。盗窃和泄漏数据会造成损失。产业间谍虽难以量化，但Juniper Research公司预计，截至2019年，全球因数据漏洞而消耗的成本将达到2.1万亿美元。至2020年[7]，每个企业因数据漏洞产生的平均成本将超过1.5亿美元。Nortel便是一个典型案例。作为世界最大的电子通信设备制造商之一，Nortel在2000年经营达到巅峰，员工近10万名，收益约达300亿美元。然而就是这样一家大型企业，仅在9年后就宣告破产。Nortel以及其他公司的的安全处部长们皆把Nortel的巨大失败归咎于中国黑客，他们认为政府资助这些黑客连续盗窃IP，致使Nortel破产[8] 。新闻报道称，这些黑客直接获取了企业高层管理人员的邮箱账号和文档。

我们时常能看到类似的网络安全威胁。2013年，雅虎因数据漏洞损失了30亿个账户的信息，至今仍是史上影响最严重且广泛的数据泄漏[9]。数年来，在公开任何用户有关信息或重置用户的账户密码前，雅虎一直很注重避免数据泄漏。2014年，索尼影视娱乐有限公司泄漏了100TB的数据，其中包括邮箱、密码、社会安全号、金融资金、市场营销计划书和四部尚未上线的索尼电影等[10] 。2016年5月，黑客入侵了美国总统候选人希拉里·克林顿的竞选主席John Podesta的邮箱[11]。其信件内容被披露在维基解密上，成就美国历史上最跌人眼球的大选冷门。

最令人担忧的是，通信和金融数据如今正逐步被极少数组织掌握控制。全球每年有数万亿封邮件被发送，而仅谷歌、苹果和微软这三家公司的客户便会收到其中超过85%的邮件[12]。诸多案例表明，这些大公司的利益与客户的福祉是相互冲突的——它的利润来自广告商，为广告商服务的同时会阻碍为客户谋求福祉。当用户不为服务付费时，他们便不再是客户。而他们与个人数据则成为了被交易的商品。

L2inc的Scott Galloway这样描述此问题：“当Facebook寻求收购WhatsApp时，他们向欧盟的监管者们确保，两家公司短期内不会共享数据。这减轻了监管者们对用户隐私会受到侵害的担忧，因而收购事宜获得允许。然而没想到，Facebook极快地找到了让数据摆脱孤岛状态的方法。”欧盟在向WhatsApp支付190亿美元后，罚款Facebook1.22亿美元。“这好比因为没花费100美元付15分钟的停车费，而要再付10美元的违规停车罚单。”[13]

几乎每种人类活动都包含沟通。因为上述所提及的诸多威胁以及正吞噬世界的软件，个人和机构隐私的基础正受到威胁[14]。随之而来的是任何关于主权或自治权的理念。这些结构性缺点也许会威胁到个人生命、商业、行业、经济甚至是国家，但确实存在解决方案。将新兴技术如密码学、分布式账本技术和代币经济等结合起来，就可以保护未做防护的数据，所有参与者也能完全控制他们自己的通信。

现有协议和服务存在的缺点

尽管如今的网络服务比之前的大众媒体技术更加去中心化，构建这些网络服务所需要用到的协议、服务和其他工具易受到中心化的控制、监视和操纵。完全去中心化的应用程序则能避开这些缺点，它需要的是好几层的替代性服务。

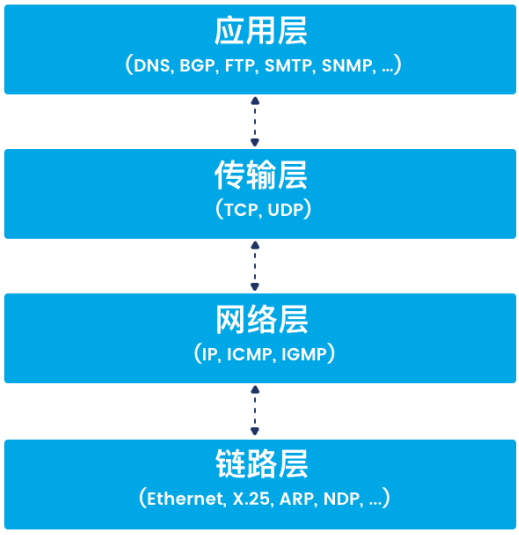
人们常见的数据交换的方法最终发展成了互联网，当时它仅用于各种大学和其他政府机构之间的数据交换。同理，万维网建立初衷是为了共享科学文献。这些技术在之后的衍变中远远超过了它们最初的用途。

1995年互联网商业化后，新企业开始改动协议来开发出各自的产品与服务。这不仅推动人们接受互联网协议，也推动这些企业成为连接顾客和互联网协议的中介，在更高的层级中收获价值。如今最大的互联网公司诸如谷歌和Facebook主要利润来源于广告。它们用激励机制保留各自用户群。终端用户已对自身数据失去控制，只能受限于掌握着他们数据的应用，使用其提供的服务。

网页协议中缺乏平衡的激励手段，这让企业越来越可能利用协议牟利。过去即便不考虑用户隐私和数据安全，网络协议也能构建起来。在过去的环境中，网络节点间互相高度信任，这恰恰是现如今互联网所缺少的。

技术挑战

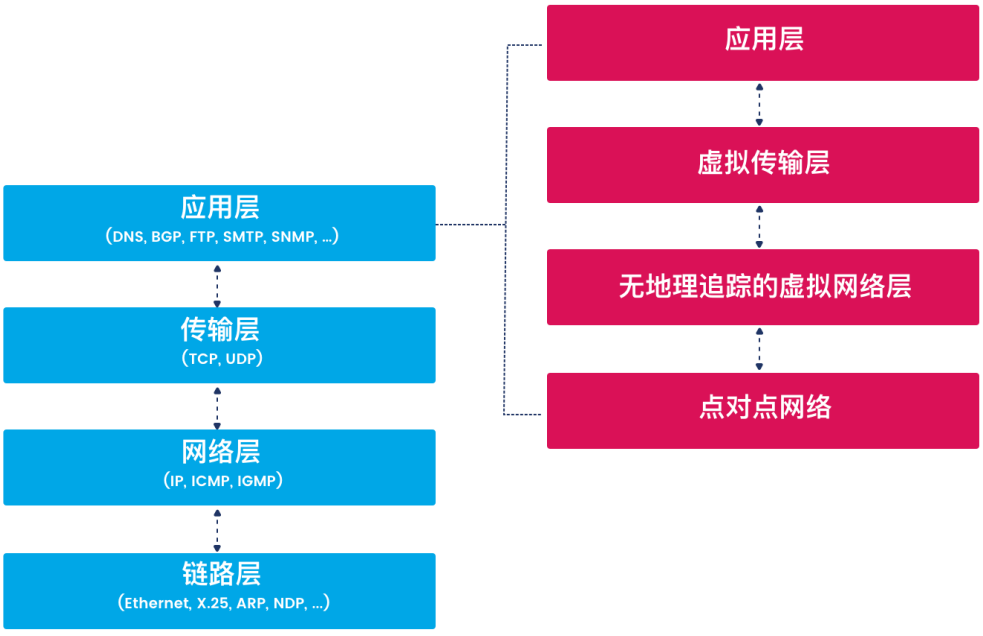
理解如今互联网存在技术瓶颈的一个难题在于，许多网络层中存在不少缺点，要解决这些缺点需要考虑多种方面，且要对各种网络层有深度理解。更近一步地仔细研究互联网协议群，即互联网所依赖的网络协议栈，将能帮助我们理解难题[15]。如下图表描述了数据在互联网上传输必须要经过的协议层。每层都依赖于下一层的服务和技术。



网络协议群

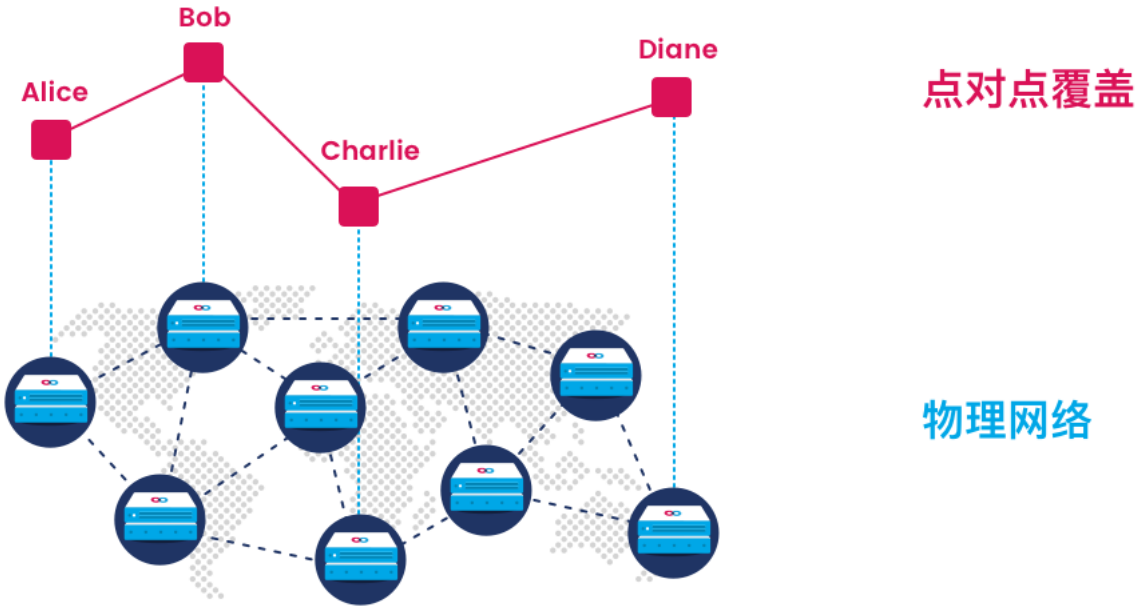
寻址

举个例子，在网络层，需要用IP地址将数据包从一个目的地发送至另一个目的地。所有互连的计算机都能通过一个公有IP地址或用公有IP设置的代理连接到互联网。IP地址的地理位置通常能精确到块级。每个网络服务提供商（ISP）负责不同范围的IP地址，使当局能轻易获取互联网用户和身份信息。通过填写对ISP的撤除通知，服务器及（或）其内容通常会断开网络连接。



去中心化的网络在网络协议群上增添虚拟抽象层级

点对点的网络可以实现完全去中心化的寻址。在点对点网络创造出的抽象层上，节点的地理位置无法轻易确认，它们也就难以被定位。



点对点网络创造出一个虚拟覆盖网络，可隐藏深层物理网络的拓扑结构

域名解析

实际网络通信还具备一个基本特征，它能够将网络地址与不易忘记的文本联系起来。域名系统[16]（DNS）所发挥的正是此功能。域名注册由非盈利组织ICANN[17]管理。其总部设在美国加利福尼亚，其利益相关者来自全球。依赖于域名系统的服务易遭受破坏，破坏来源可能是对利益相关者有诉求的个人和组织，也可能来自政府和企业，它们控制基础架构、篡改DNS响应或公开发布代替性的DNS记录。在这样的情况下，如果管辖区域的国家想查禁任何基于互联网的消息，使用DNS和（或）发布撤除通知可以轻易阻止消息传播。而去中心化的应用程序通过提供基于区块链的代替性域名解析协议，可以消除此类传播壁垒。

证书授权中心

与域名系统相关的是传输层安全协议[18]（TLS）以及TLS对证书授权中心（CA）系统的依赖性问题。因证书授权中心必须获得完全的信任，它也变成了失败的集中发生地，是被攻击的主要目标。即便是新兴的去中心化基础架构，也不得不持续地依赖于此证书授权中心系统。EtherDelta是世界上最大的去中心化数字加密货币交易平台之一，就因其DNS账户受黑客攻击而被盗[19]。域控制器是给证书授权中心的凭证，为了让CA生成域名证书。返回该网站的用户随后获得一份正确域的有效HTTPS证书，因此当他们遭遇恶意网页服务器时，浏览器内他们无法受安全检查的保护。据该网站的一些用户反馈，他们在遭受黑客攻击后损失了巨额数字加密货币。

许多其他受信任的机构已经遭遇网络诈骗。在那些诈骗案例中，恶意分子生成由受信任的CA签发的有效证书，但该证书的域名只是看似一样，却带有木马的源代码。而那些诈骗犯能成功从受信任的证书授权中心获得有效证书，这说明当下系统存在安全问题。目前对去中心化的身份和信誉系统的研究正在开展，以便能为用户提供比证书授权中心系统更高水平的真实性保证。

邮件协议（SMTP/IMAP）

传统邮件经过简单邮件传输协议[20]（SMTP）和互联网邮件访问协议[21]（IMAP）会变得略微去中心化，具体表现在任何人都能设置一个邮件服务器，发送邮件。在邮件协议诞生的那个时代互联网迅速发展，所有节点都被信任，且没有内置的安全机制。由于发送未经请求的信息几乎不消耗成本，这就纵容垃圾邮件猖獗一时。尽管如域名密钥识别邮件[22]（DKIM）的扩展技术能帮助减少垃圾邮件，SMTP和IMAP也依赖于DNS和传统的客户端/服务器架构，因此它们并不完全去中心化。SMTP和IMAP也无法做到实时响应，所以用户期待Slack和WhatsApp这一类消息软件可以做到实时通信。无论如何，SMTP默认设置并非端到端加密，而且加密解决方案对于非技术性用户来说并不容易。

群通信协议（IRC/XMPP）

网间实时聊天[23]（IRC）和可扩展消息传递和到场协议[24]（XMPP）属于更受欢迎的第一代互联网群通信协议。这些协议允许随机服务器分布，却仍依赖于DNS和传统的客户端/服务器架构，并未完全去中心化。

主机电子邮件

尽管人们能自主运行他们的电子邮件服务器，并用PGP加密[25]，却很少有人会这么做，人们大多依赖主机电子邮件平台，如Gmail，iCloud，Outlook，雅虎邮箱等。除去SMTP所包含的所有缺点，这些服务依靠第三方基础架构，无法控制用户的数据，并且需要提供此服务的机构无理由给予高度信任。对于支持自定义域的服务如GSuite，还需要来自域管理员的信任。域管理员有权获取并监视所有域用户的通信。

持有数据可能会使某些企业用户获利，但它同时也承载了额外负担。保有数据的公司也许会违背自身及客户的利益，被迫地使用其保留的数据。例如在2016年，苹果公司就被要求协助美国联邦调查局[26]（FBI）破解一部苹果手机。尽管有人认为这种特别请求有利于公众利益，它却引发了许多其他苹果用户的忧虑。其他用户担心如果此种干预成为常态，隐私和公民自由可能会受到威胁。苹果公司以保护用户利益为由拒绝了FBI的请求，并表示若为FBI提供它们产品的后门，此行为容易让恶意黑客有机可乘，而且FBI的请求已经构成了政府越权。其他政府机构也对知名的通信应用软件，如WhatsApp[27]和Skype[28]，发出过类似请求，希望在安全加密方面开后门。限制获取用户数据的途径将企业责任降至最低。

聊天

如今许多第三方服务为机构提供便捷通信平台，满足公司同事之间的实时交流，聊天格式更加丰富，同时支持文件共享和远程监控功能。这之中最富盛名的是Slack，它拥有六百多万名用户[29]。在客户享受服务提供商的便利和丰富特性时，该服务提供商也能看到客户的个人数据。客户必须信任该服务提供商，才能保护它，并令其流畅地运作。举个例子，在2018年1月9号这个工作日，Slack上引发了一场群愤，卷入了数百万名用户。其用户用社交网络抒发愤怒，使该事件占据推特热点话题榜榜首[30]。完全去中心化的通信能消除这些失败。

加密点对点/群组聊天

最近由Keybase、Signal和其他一些公司发布的产品，可以在某些场合为个人甚至群组提供全加密通信。不过他们要依赖中心化的基础架构来运营或存储客户数据，因而会令客户面临数据丢失、服务中断等问题。而这些解决方案虽比其他某些解决方案能更好地保持用户主权，却仍需要作出很多妥协，并且可能让客户遭受一些不必要的风险。

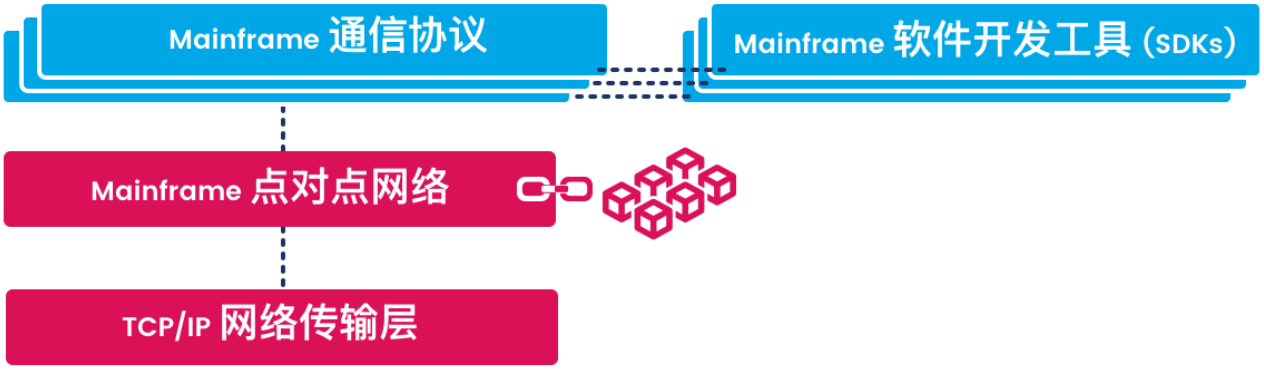
分布式私聊

一些像Matrix这样的机构开始允许用户基于其租赁的云基础架构而非第三方基础架构，来主控自身通信，从而进一步强化用户主权。我们坚信这一步的方向是正确的，但这仅仅是个开始。完全去中心化的通信需要无主机架构，即整个应用程序基础架构在受激励的点对点协议上运作。

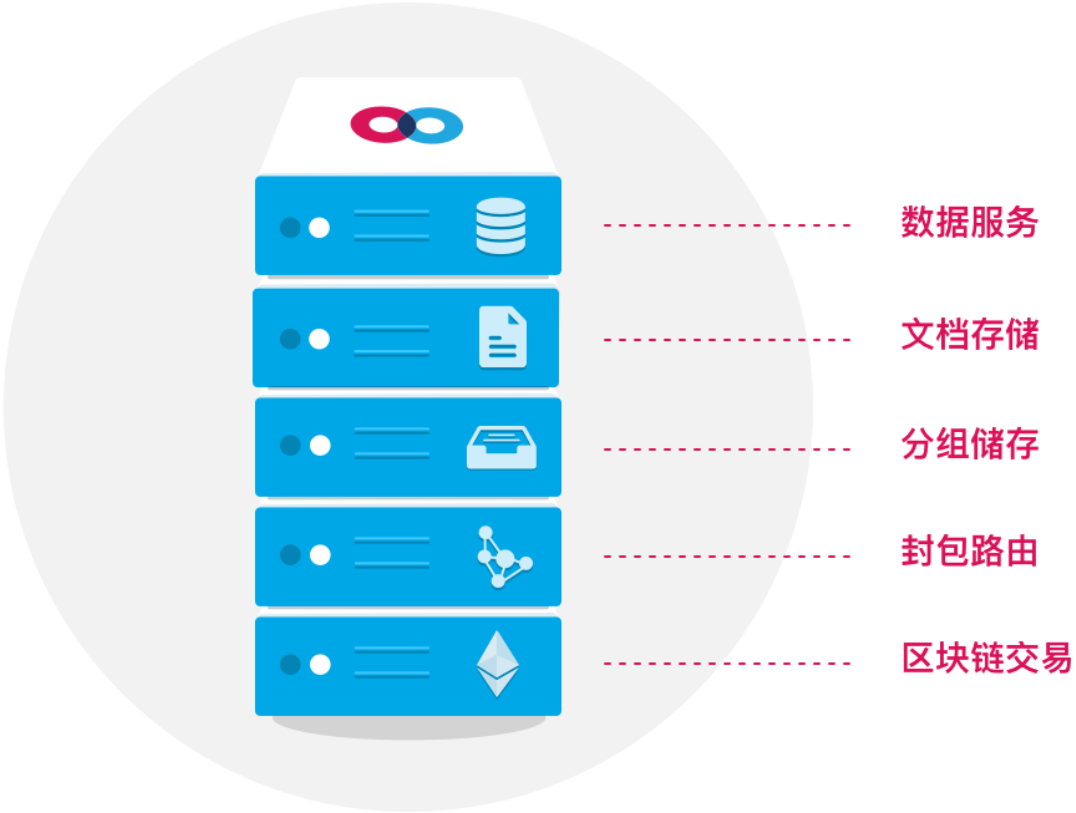
一个势不可挡的通信平台

Mainframe是一个势不可挡的平台，它融合了如今最佳网络协议和应用程序的优点，同时具备最高级的安全保障和用户主权。这一平台包含了多种协议和传输层，受到代币制激励。在此平台上，用户还能享有一系列常用语言的软件开发工具（SDKs）、操作系统、设备和代币交换的智能合约和预言机，体验到同各种区块链协同工作的便捷。

在最低层级，Mainframe包含一个基于Kademlia[31]协议的点对点网络，用于区块链交易的传播与执行。从这一网络层抽象出的网络传输层正是网络层所依赖的，可追踪地理位置，并随机为每个点对点节点或节点分配地址。在此网络中，运用区块链代币可实现节点间价值的交换。为保障安全通信，Mainframe还为该传输层提供另外的协议 。



每个Mainframe节点会包含多个P2P服务应用层接口，包括区块链交易、封包路由、数据包持有、文档存储和数据服务接口。每项P2P服务都完全由点对点用户提供，它们在受激励的点对点合作中运作，毫不依赖于任何第三方基础架构。

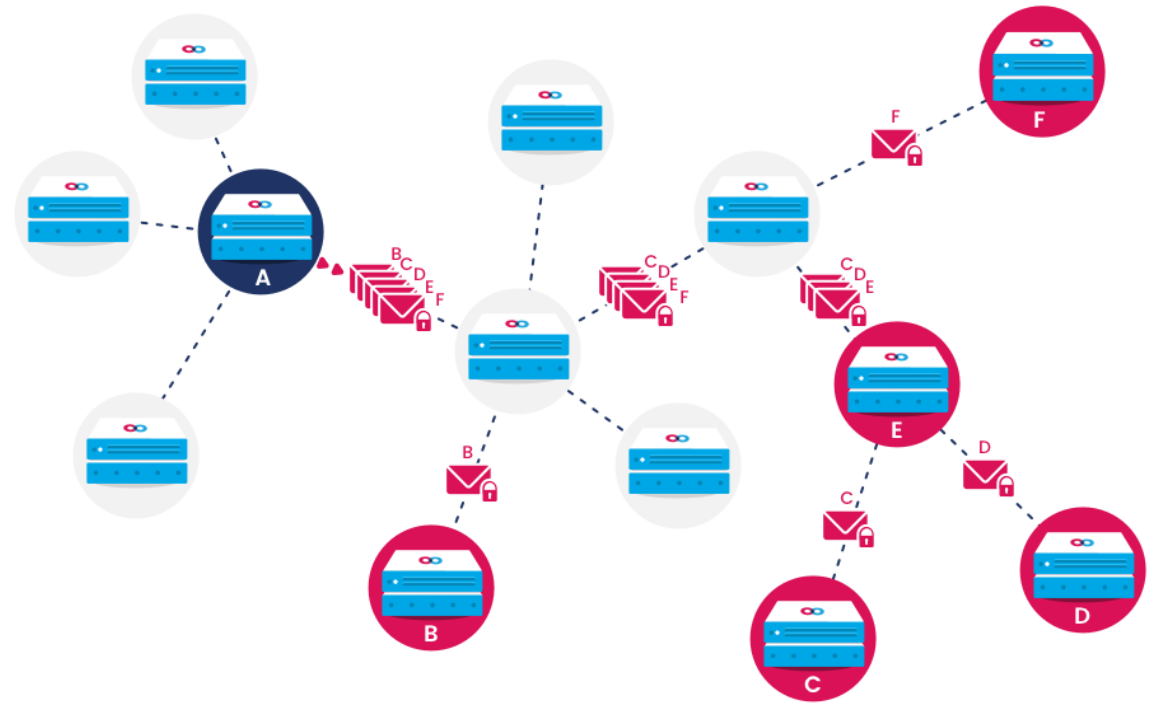


Mainframe 节点
概念图

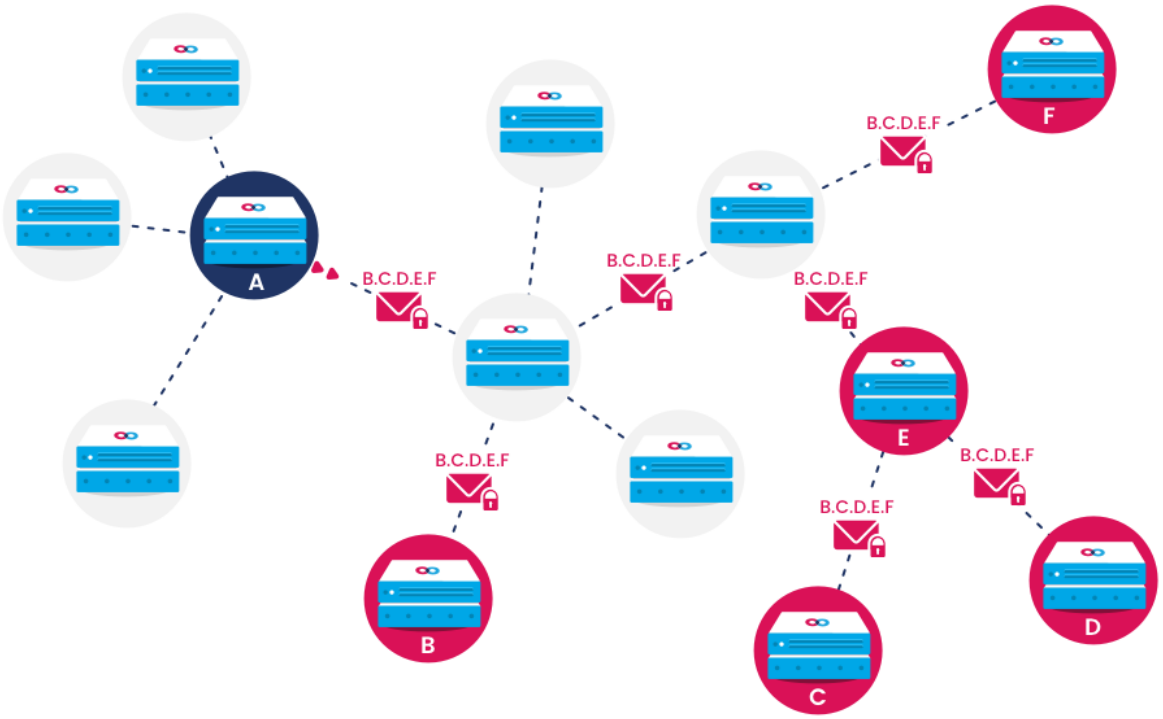
加密

Mainframe提供一对一和一对多加密协议。每个Mainframe节点都有与之关联的一个非对称密钥对，用于解密发送给该节点的数据包。当某节点要向另一节点发送数据包时，它或使用接收方节点的公钥给数据包加密，或使用预先定下的共享密钥。另有额外的对称密钥保障前向保密。接收方节点的公开密钥有两种获取方式：1. 从联系信息的前一次交换中获取，例如采用交换通讯信息这种带外联系；2. 从个人间公共密钥的直接交换中获取。数据包加密是Mainframe传输协议至关重要、无法避开的一部分。

组播模式中，数据包能发送给多个节点。发送方即组播数据包的发送节点，便能只发送单个数据包而不必为两个或两个以上的接收方复制数据包。Mainframe提供共享密钥协商协议，使发送给多个接收方节点的组播数据包只需加密一次。这种运营模式面向需要中等安全级别的高性能应用程序，多个目标地址包含在数据包元数据中。该模式还可以与暗路由相结合（下文将具体阐释）。



非组播模式，节点A向节点B、C、D、E和F发送数据包

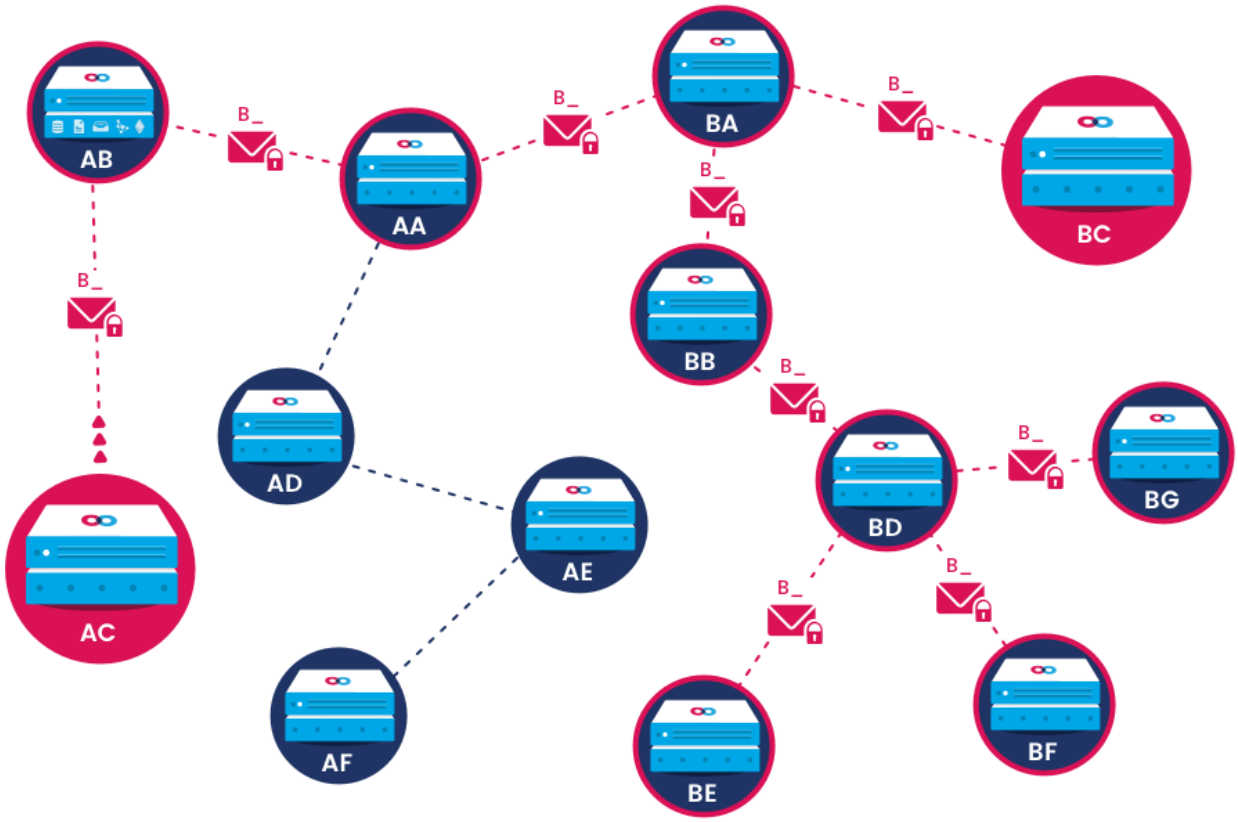


组播模式，节点A向节点B、C、D、E和F发送数据包

组播模式中，发送给一批节点的同样信息只需加密一次，且无需复制数据包便能传遍整个网络

暗路由

传统网络系统，尽管使用了加密技术，却仍会给恶意分子可乘之机，收集网络中的具体通讯信息。Mainframe使用可配置的暗路由，能有效在节点间防范此种情况。该暗路由建立在Holbrook对PSS协议的研究上。PSS协议[32]本身衍变于Whisper协议，该协议最初由Wood提出[33]。在暗路由模式中，每个数据包接收方节点的地址都能匹配上部分公开的目标地址。数据包能有效地在这些节点中得到传播，但最后它会分布至每一个匹配上的节点，从而该区域内任何网络监视者都无法追踪某个特定的数据包接收方节点。



节点AC借助暗路由（部分寻址）向节点BC发送数据包。
该数据包会发送给可匹配地址的所有节点，但只有节点BC能破解数据包信息。

当为数据包寻址时，节点负责挑选合适层级的亮度（即地址特性）。地址特性过多将增大恶意分子识别出节点间通信模式的可能性，而地址特性过少则会加大拥堵和传输成本。Mainframe能够根据具体的网络情况和隐私要求，为不同用户提供特殊算法，确定合理的地址特性设置。

因为数据包不需要完全定址，会话管理变得更具挑战性。节点必须能有另外一种途径找出它们有兴趣查看的数据包。而这可以通过使用数据包内之前便意见达成一致的主题ID实现。Mainframe提供会话管理协议，帮助应用程序追踪并发起多个数据流。当单个节点或一批节点间产生新会话时，主题ID便生成，并在所有会话参与者中私密共享。参与者便能用同一主题ID获取这之后发送的数据包。

倘若节点所选择的主题ID正被其他节点使用，该节点随后可破解的数据包必定由一个已知的秘密密钥加密，且该节点将忽略拥有相同主题ID的其他数据包。正是如此，主题ID不仅帮助减少节点对无关数据包的处理超负荷，还完美地解决了封包碰撞问题。当多个不同类别的通信流都使用同一个主题ID时，截收者想要识别通信模式就变得更加困难。

因为在此运营模式中，通信模式无法被轻易识别，网络高度防范监管，阻止对特定拒绝服务节点进行定位。Mainframe将加密技术与暗路由相结合，使网络安全真正达到前所未有的高等级。

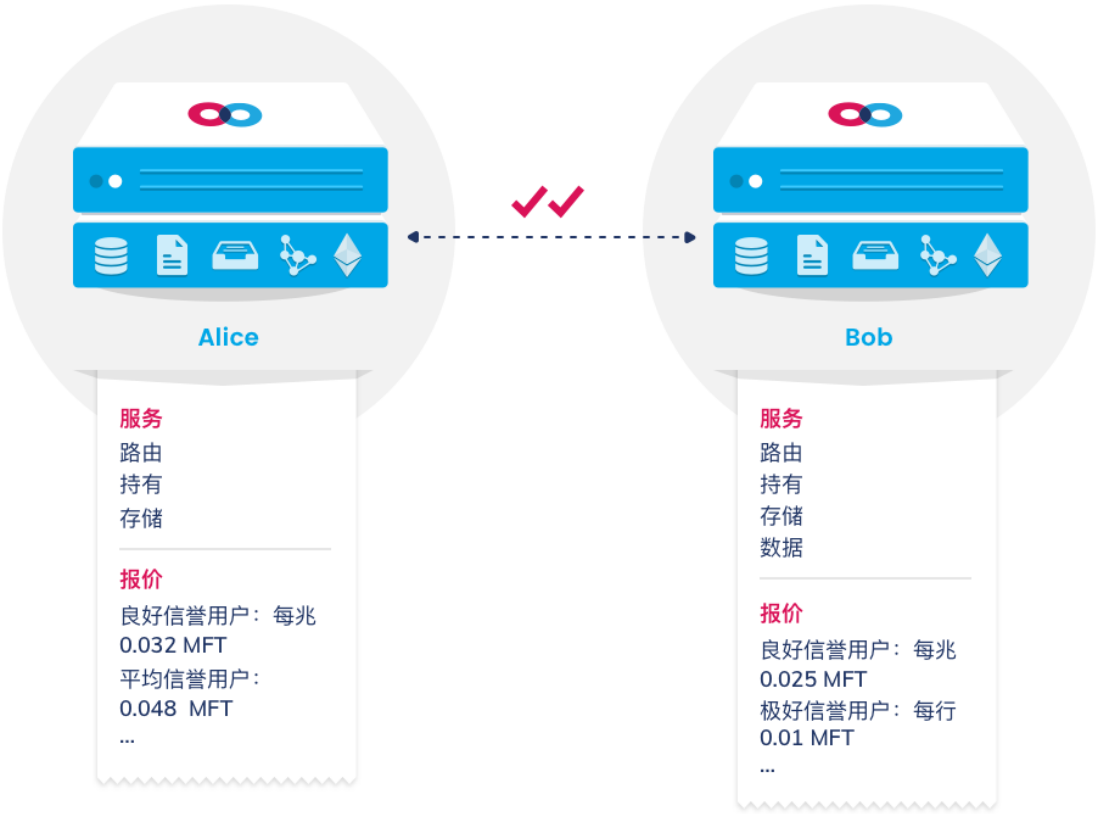
奖励模式

Mainframe通信使用并建立于一个服务提供广义激励模型，也被Trón和Fischer称为“交换，保证和欺骗”[34]。此模型用于奖励网络节点提供的各种重要服务。

奖励封包路由

点对点节点间签订协议为彼此提供服务，即保障稳定可靠的数据包接收和发送。它们使用SWAP协议对彼此间发送和接收的宽带作记录。

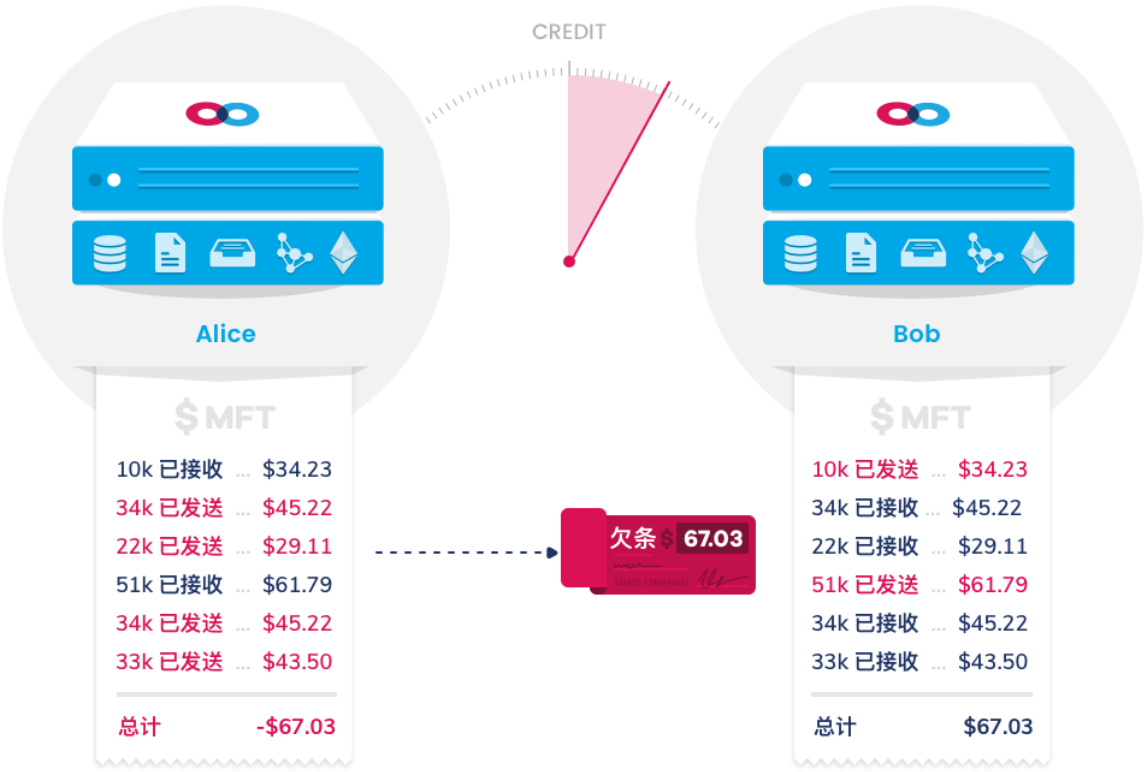
SWAP协议中每个参与的节点都使用支票本智能合约来管理服务计算过程，并将资金以ERC20代币的形式存入合约。Mainframe代币（代码：MFT）是其节点间交易的手段。节点借助服务发现协议来发布它们所提供的服务和价格。Mainframe中各节点可协商并同意服务、价格和交换媒介，这大大提升了网络的公正性和协同工作能力，也让更多的股东有更加强烈的意愿加入。如果潜在点对点节点能接受服务定价，它们便会发展成为同级关系。



Mainframe使用服务发现协议，
确定每个节点的服务和价格

当某节点点对点方所提供的宽带数量超出特定阈值时，该点对点节点会开出一张“发票”再次请求资金输入。享受服务的节点则会开出一张“支票”给点对点节点，利用加密技术签署一份数据，将信息输入支票本合约中。节点也许会立马兑现支票，也有可能该节点最终可以抵消那笔费用，便暂不兑现支票。如果确实发生这种情况，该节点也许只需把之前那张支票作废，便可将它与点对点节点之间的账款“一笔勾销”，或者它也可选择另开一张支票。在每个节点清算其产生的账目前，它收到支票的有效期存在一个可配置的阈值。支票的交换在链下完成。这增大了违约风险，但也令参与者的交易成本比寻常大大减少 。

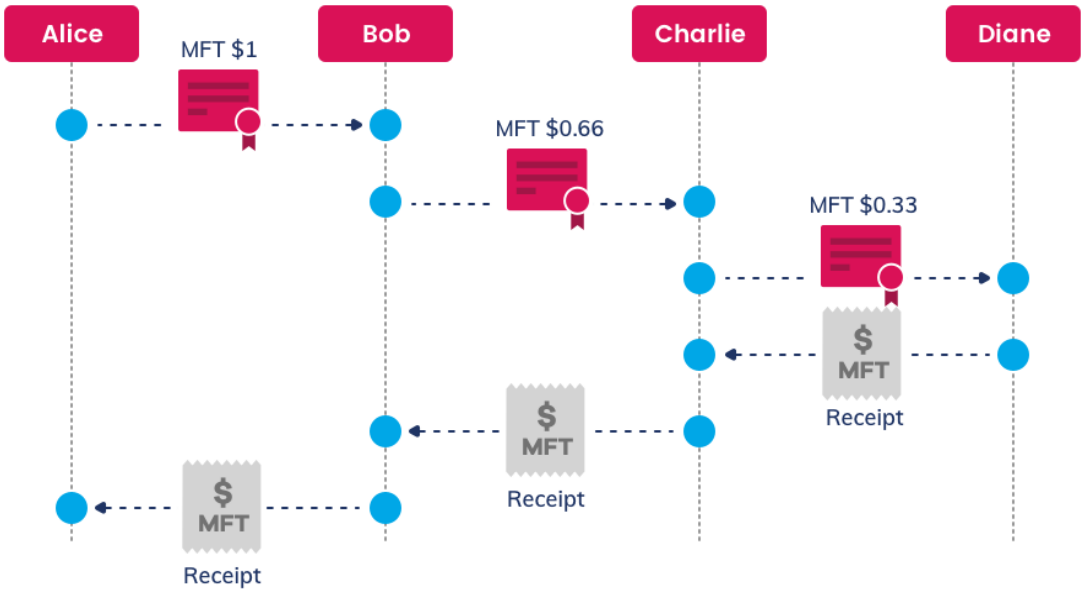
支票能否能被支付并非定数。倘若一个节点试图用代币兑现支票，可支票本合约中却没有足够存款，那么为其提供服务的节点会遭受损失，不过该节点也会因那张空头支票名声受损，最终它将被禁止加入Mainframe网络。倘若一个节点无法在为其提供服务的点对点节点所宣布的截止日期前开支票，或开出了空头支票，这些行为会被记录在区块链的总账上，并对其他所有节点可见。



使用Mainframe的信誉评分API，节点能从其他节点获取信誉分，甚至可以把按照它们自己所设立的评分标准得到的分数计算在内。历史较少或没有历史记录的节点分数中等。当它们按时缴费，或向账户中充值时，分数增加，反之亦然。每个节点对于信誉分不同阈值的定价会展示在其服务发现中，而一个节点甚至还可以与信誉分过低的点对点节点彻底切断点对点关系。

奖励数据包投递

Mainframe的点对点节点间存在直接经济关系。同时，它采用加密认证投递的概念，鼓励在网络中多个点对点的跳距间发送数据包。此运营模式中的发送方节点会发布一张有条件的契据，特别说明一个第三方托管委付条件，即一些数据应当来自接收方节点，以证明数据包成功递送。唯有以此种方式认证一部分数据包，服务的性能与稳定性才能取得平衡。



Alice向Diane发送数据包，同时附带了一份认证发送的契据。每个节点收集到一定份额的契据，便将数据包传送给另外一方，点对点节点在收到数据包后将发回一份收据，证明递送成功。

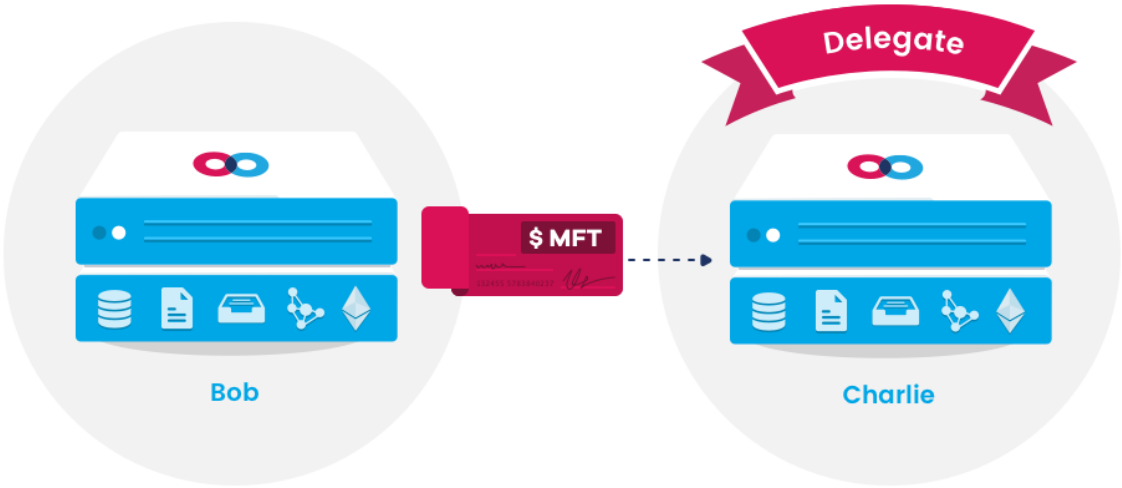
每个节点可以出示从其毗邻节点那获取到的收据，以证明数据包接收成功。每个节点也能在确认数据包发送后，要求毗邻节点出示类似证明，从而证明数据包已被成功传达至毗邻节点。无法出示已传达证明的节点必须做到以下两点中的一点：1. 证明接收方节点当前离线；2. 证明它们使用Kademlia地址，且很有可能与接收方节点距离最近。否则，认定该节点数据包递送失败，予以批评并没收递送时交付的代币。这一过程被称作指责[35]，严格确保了数据包的安全送达。

在暗路由模式的每个跳距，一份契据只发送给随机抽选的一批毗邻节点，而非找到所有匹配地址的节点验证其是否完成数据包传送。因此Mainframe就能提供合理奖励使数据包传输安全可靠地进行，同时也使接收方节点保持匿名。在暗路由模式下，因无选择复制数据包，受奖励的数据包递送会消耗更多成本。网络推理使发送方节点能根据它们的亮度（即地址特性）设置和毗邻节点选择算法的配置，估算出发送数据包将要耗费的费用。

奖励数据包持有

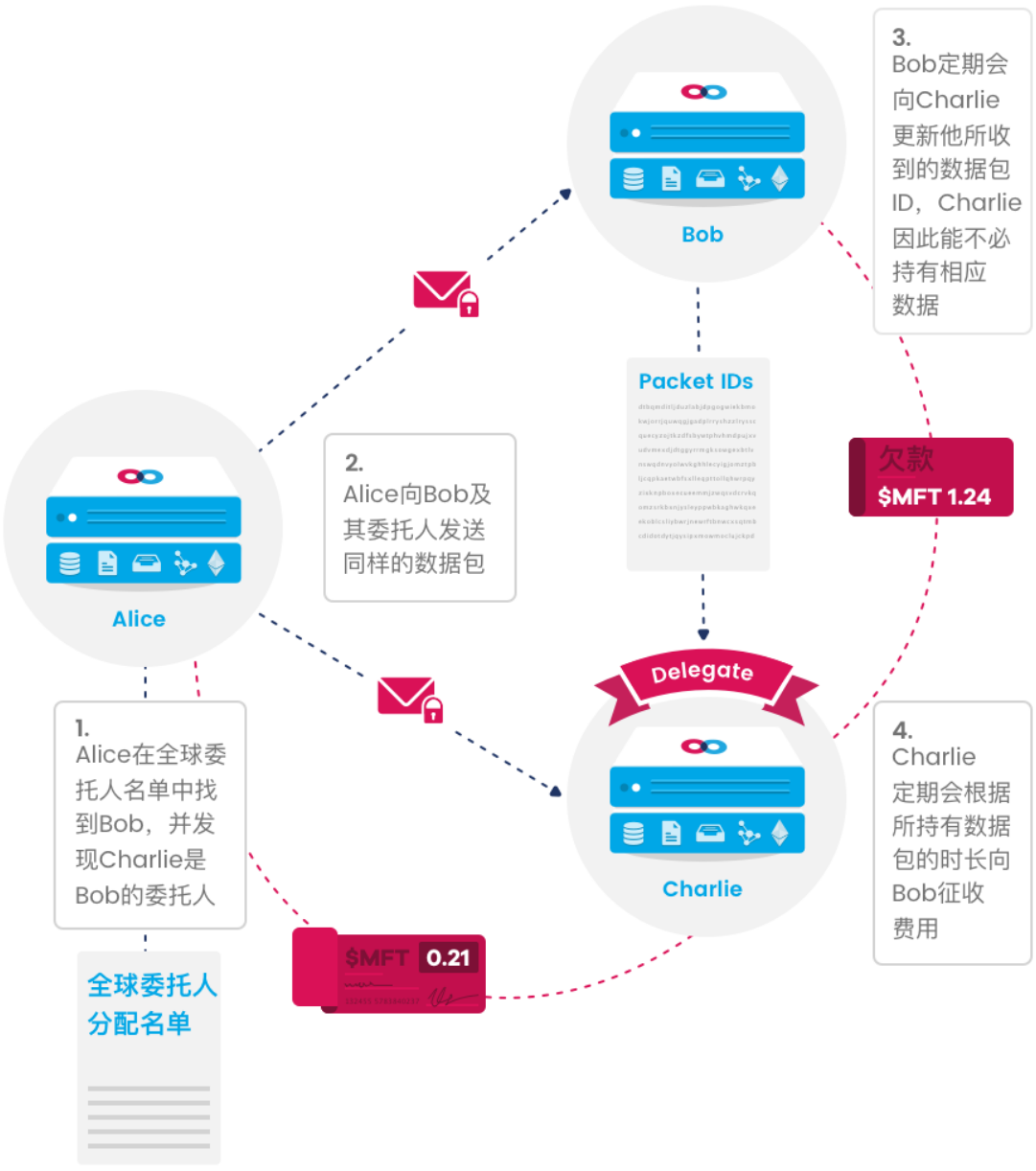
即便一些节点掉线，Mainframe通信也必须继续运作。Mainframe的基础架构完全建立在点对点网络中节点所提供的各项服务上。正因如此，一些使用案例会要求，发送给某离线节点的数据包，在该离线节点重新在线前，必须由其他节点暂时持有。这项服务受到奖励。

节点也许在其服务发现协议中会写有包持有这一服务。其他需要此服务的节点，在发送服务发现请求后将以可接受的价格，匹配到提供包持有服务的节点。一旦它们找到合适的包持有委托方节点，有服务需求的节点便与委托方节点签订了服务协议。且使用数据服务接口，能在全球包持有者信息表上更新它们的包持有委托方名单。此时根据服务协议，为防数据包无法被安全保留，委托方节点也需付上一定金额的代币。



在节点离线时，它或将付费请委托方节点持有数据包

在向其他节点发送数据包前，首先必须查看全球数据包持有者信息表，确认数据包接收方节点是否有委托代表。如果有，发送方节点不仅要给接收方发送数据包，还必须向接收方的所有委托人发送数据包。接收方会有一份近日已接收过数据包ID的签收名单，据此它会定期向所有委托人更新数据包接收情况。委托人则可能将已成功签发的数据包从它所持数据包的队列中删去，并根据它们为发送方节点持有数据包的时长收费。离线一段时间的节点也可能向其委托人请求被持有的数据包。

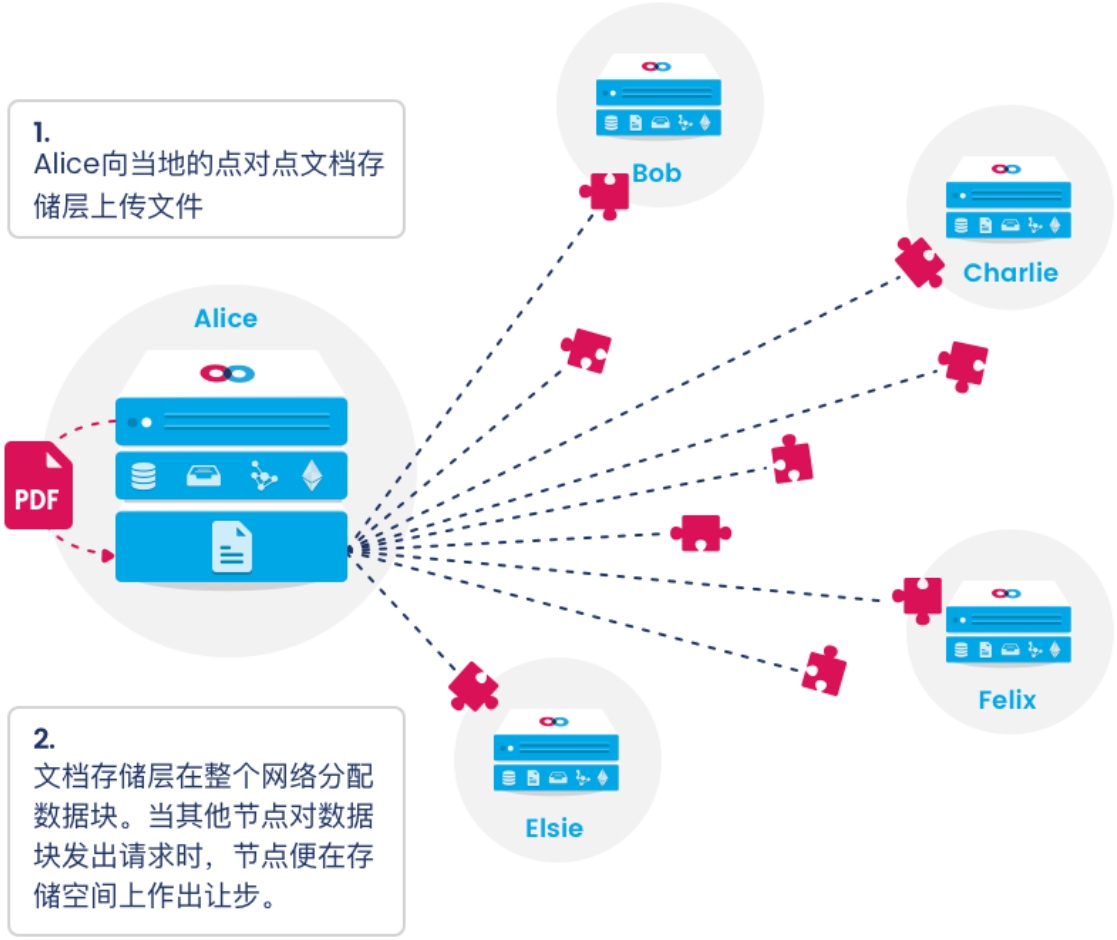


找到委托方可确保节点离线时由委托者持有数据包，
以便该节点之后取回数据包

如果委托人有违反其服务协议的嫌疑，欺骗合约可对其立案审理。该合约扮演执行法庭诉讼的国家机器一角。根据被传召目击者的证词，合约将判定该委托人有罪/无罪。被证明有罪的委托人将被没收它们之前存入保证合约的资金。欺骗合约的判决将被记录在链上，且能用来量化评估一个节点的信誉。

奖励文档存储

Mainframe在封包路由环节使用“交换”阶段，在受奖励的文档存储层则采用服务提供的“保证和欺骗”两个阶段。节点证明（保证）所存储的是一份文档的随机部分（数据块）。由于它们也可能通过不了存储测试，节点押下一定数额的代币。而后系统会定期请求节点出示一份它对任意某个数据块的存储加密证明。如果节点无法发回有效数据块，合约可能向其发起欺骗诉讼，被证明有罪的节点将损失所押代币。当文档数据块被其他节点请求，存储节点能获得代币奖励[36]。



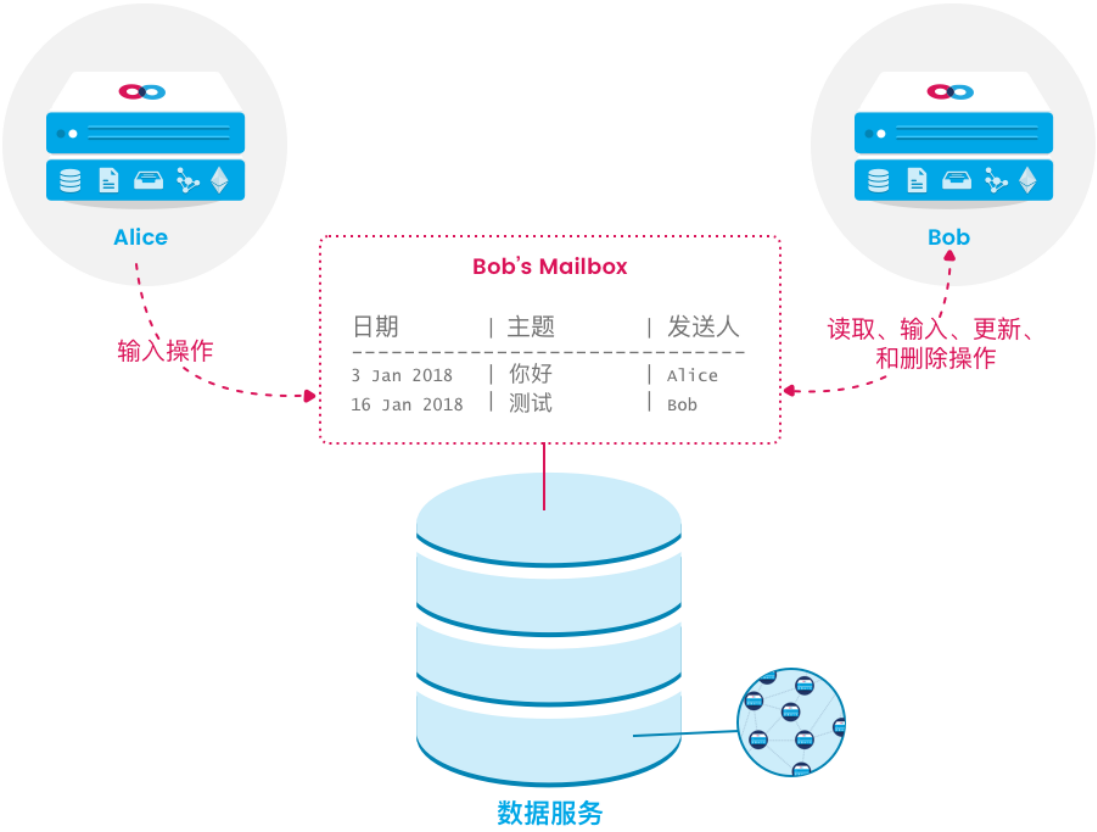
奖励数据服务

尽管许多使用案例得益于文档存储，该服务却不足以加载和保存随时会做修改的大型文档。应对此类情况，Mainframe提供受奖励的数据库服务。

期望以此类服务赚代币的节点会使用服务发现协议做宣传。其他节点则也许会存储变址数据集，以应对随后的数据收回和请求。这些数据集的存储具有冗余性，可指定用户 。冗余性越强，当数据

不幸丢失时，该节点所能获得的赔偿便越多。在欺骗立案的作证环节，当被请求的数据无法被提供时，目击者证词最终可能令数据提供方所押的代币被没收[37]，从而保障此服务可靠且受到奖励。

数据集拥有者能指定节点，从数据集中读取、输入、更新和删除行。此种细粒度的权限控制使许多应用程序特性得以发挥作用。例如，任何用户（或者说，任何之前获得授权的用户）能借助邮箱功能，向代表其他用户邮箱的数据集插入行，但只有邮箱主人才能从该数据集中读取、更新或删除行。拥有读取特权的用户可以订阅通知，实时了解数据集发生的任何变化。



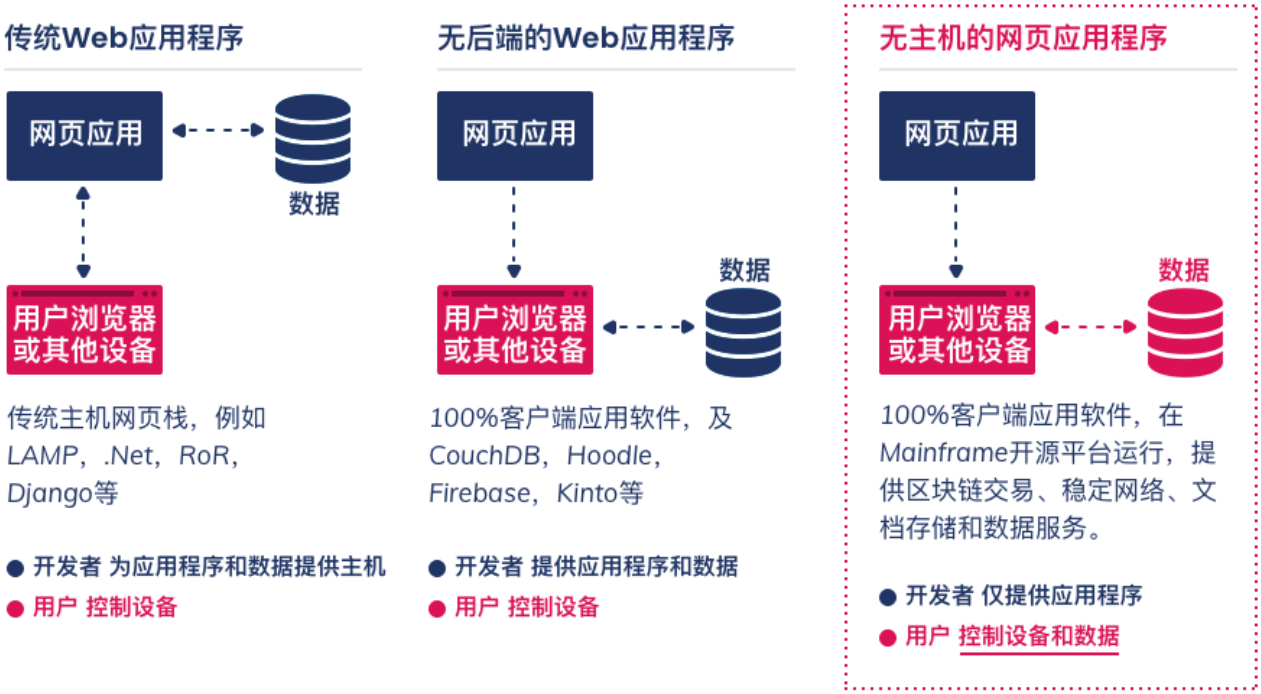
以上是使用Mainframe数据服务的应用程序案例。Alice能向代表Bob邮箱的方框写入新信息，却无法读取或变更邮箱中的信息。Bob作为邮箱主人，能读取并修改邮箱中的信息。Mainframe数据服务层确保网络中存储着这些数据集的多个备份，保障服务性能和高冗余性。

无主机架构

Mainframe保障的网络弹性体现在两个方面原因：分布式和去中心化。分布式网络如今相对常见，它更多以内容分发网络（CDN）的形式出现，为人们提供高度可用的权限获取网络内容。在这种架构下，即便节点子集遭受损失或攻击，网络也能照常运作。Mainframe网络的分布式特征意味着，在网络参与者加入、离开之际，网络有增长和自愈能力。随着网络规模的扩大，任意两节点间可能存在的路由路径数增加，这将耗费潜在热点，并会大大减少节点退出对网络健康带来的总体影响。为维持一个最佳的覆盖网络，Kademlia网络协议将确保，节点在其点对点节点掉线后能努力寻找新路径。

依据定义，去中心化的网络没有中央集权以掌控其中的数据流。那么当网络中不存在任何失败或攻击面时，潜在恶意方要关闭网络就变得极其困难。比特流（BitTorrent）的运营正是基于这种网络。尽管有关torrent内容的宣传网站被法庭指令关闭，它所依赖的文档共享网络却无法得到有效禁止。Mainframe网络的运营模式与之类似，并且任何时刻都不依赖在线或可连接的特定节点集。没有哪个实体能（即便是Mainframe本身也无法）控制或摧毁此网络的运营。

除去其弹性结构，由此网络提供的多种服务层在构建时，必须尽可能地减少对特定节点的依赖。正因如此，该网络提供的服务会考虑冗余性，在多个节点存储个人数据碎片，并指派多个节点来完成被请求的服务。网络服务层的存在是为了支持那些真正“无主机”或完全去中心化应用程序的发展[38]。这意味着，不同于他们在传统网页服务的体验，Mainframe平台上的开发者无需供应或管理他们自己的基础架构，此平台上的客户也不必信任第三方来维持基础架构。随着此空间发展愈渐成熟，Mainframe将继续开发新服务，以期更好地满足完全去中心化应用程序的需求。



协同工作能力

令所有应用程序在我们的平台上享受便捷的通信体验，是Mainframe构建的初衷。为满足开发者需求，我们将推出针对他们的软件开发工具，使Mainframe代码能在主流平台以及常用语言中运作。另外，我们也将在多个区块链上，如Ethereum，RSK和Tezos，提供预言机和智能合约，促进代币制的激励层互动 。

为努力增强开发者对我们的接受度，Mainframe除推出软件开发工具外，还关注开发者发展，提供详尽的培训教程和文献；组织并支持开发者论坛，讨论构建于Mainframe平台的应用程序及其运行问题；还提供收费服务，可做支持和咨询。

代币效用

Mainframe代币在其生态系统中发挥多种作用：

- 奖励点对点节点之间及时、有效的数据包传送；
- 奖励数据包从发送方节点至接收方节点的递送；
- 奖励可靠、去中心化的文档存储；
- 奖励可靠、去中心化的数据服务；
- 可以用作交易媒介，在Mainframe的平台市场上买卖数字商品和服务。

使用案例

Mainframe平台支持多种产品和服务。第一个建立于此平台的应用程序是通信应用程序，它充分利用了Mainframe提供的去中心化协议。该应用程序的早期版本被称为Onyx，于2017年12月19日发布。

Onyx通讯应用

Onyx是建立在Mainframe平台上的通讯应用。它为手机与PC端用户提供一流体验，支持的系统包括Windows，MacOS，Linux，iOS和Android。它被评选为“年度企业实时通信工具”。优化后的应用程序能将系统资源消耗降至最低。它支持点对点聊天和群聊，记录所发信息语境，允许用户快速在所有对话中查找内容。

可配置的暗路由

Onyx是第一个允许用户使用暗路由的应用程序。用户可以为其群聊和私聊频道发出的消息配置亮度设置。

丰富的内容和微格式

Onyx具备极其丰富的格式特性，可附件发送文件，并有支持查看图片和视频的内嵌插件。除此以外，Onyx还有许多其他简单通讯应用程序所不具备的微格式，包括投票、任务分工、群清单等等，展现出多样的交互特性。

全文检索

Onyx 从当地抓取联系人名单和信息内容，快速获取所存档信息，并能对信息内容和联系人列表进行全文检索。

名录服务

Onyx提供去中心化的联系人存储、编辑和共享服务。Onyx采用去中心化的命名服务，如ENS记录用户认为可公开的联系人信息[39]，并将该信息存储在Mainframe的去中心化存储中心。而对于个人或机构用户想要私下共享的联系人信息，Onyx则采用如uPort[40]或Sovrin[41] 账本确定网络身份，实现联系人信息私密共享。

在线和活跃状态信号提示

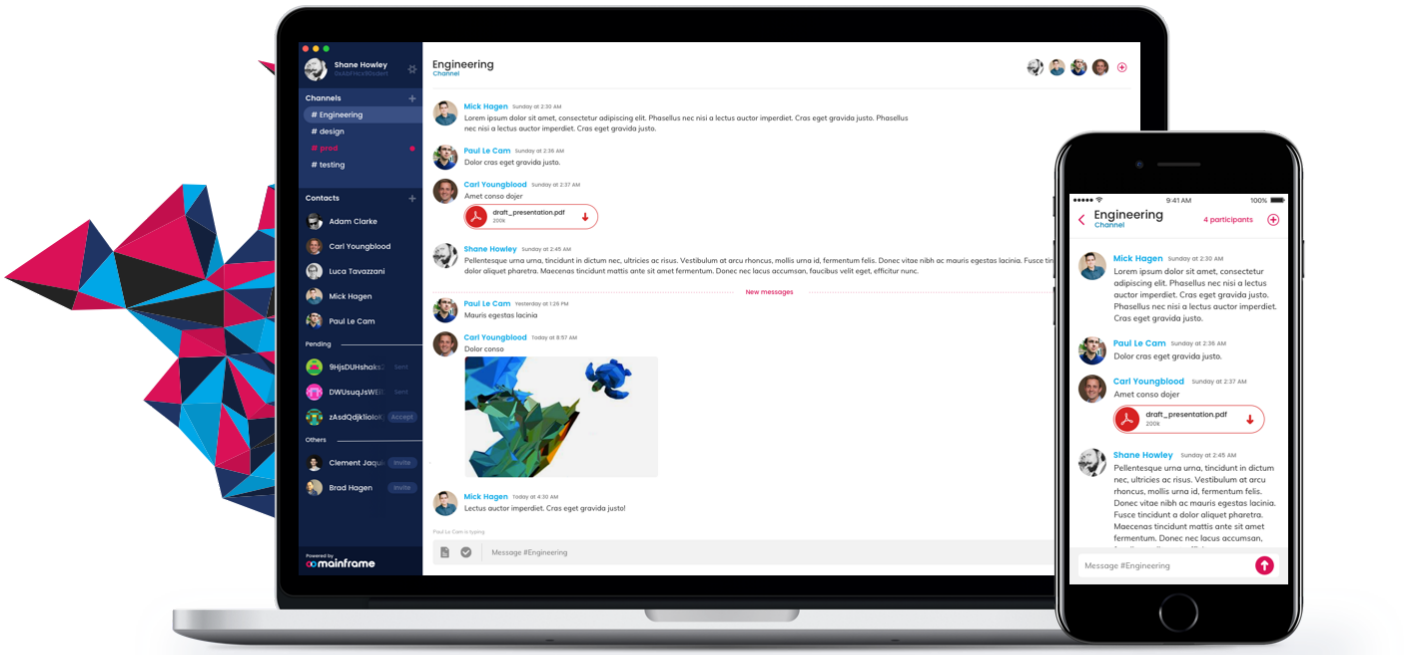
无论是在个人简介还是聊天页面，Onyx都能使用户向其他人轻松提醒其状态。例如，在聊天时，用户能看到另一名最近一次活跃的时间，或看到当前对方正在输入信息的提示。这些通知也能被取消。

聊天机器人市场

Onyx有高度延展性，支持用户创造应用程序，满足企业和个人的特定需求。创造出的应用程序能用Mainframe代币进行买卖。

成功的聊天机器人案例包括：

- 自动回复。在个人或群聊频道，听到关键词或收到相关信息后予以回复；
- 代理机。听从指令，完成领域特定的各类任务；
- 能为用户或机构提供其他基于云端和/或去中心化服务的应用程序。



其他使用案例

毋庸置疑，Mainframe平台涌现出了许多出于意料的使用方式。不过我们认为，以下领域蕴含创造力，非常适合Mainframe平台一展身手。

企业

2016年欧盟通过了《通用数据保护条例》（GDPR），要求企业的信息技术实践需要遵守严格的隐私政策。如果给予IT管理员一个注重用户主权的平台，企业能设计精简的系统，不必承受信息在传输中泄漏的风险。在稳定安全的系统中，当敏感数据被隔离时，企业应负的责任会减少。

与之类似，美国医疗信息技术职业人士使用此平台构建了遵守《健康保险携带和责任法案》（HIPAA）的解决方案。金融和学术届的专家同理也需要控制自身数据。

消费品

物联网当下非常备受瞩目，而物联网设备所引发的安全威胁也几乎受到了同等关注。带有传感器和输入设备的硬件（但更少的情况是与用户的直接交互）会成为黑客的主要攻击对象。2016年10月，美国东部海岸网络遭受Mirai Botnet攻击，致使该地区大部分人无法访问网站[42]。Mainframe的寻址和路由机制与去中心化身份和信誉层巧妙结合，有效降低了物联网连接设备受攻击的可能性。

政府

可能和众人料想的不同， 这些工具对政府同样也很有帮助。敏感信息是政府操作中的必要组成部分，机构内部和机构间的数据传输非常重要。运用Mainframe网络，机构能降低信息窃取和泄漏的风险，并防止被恶意软件感染。

社交网络和金融科技

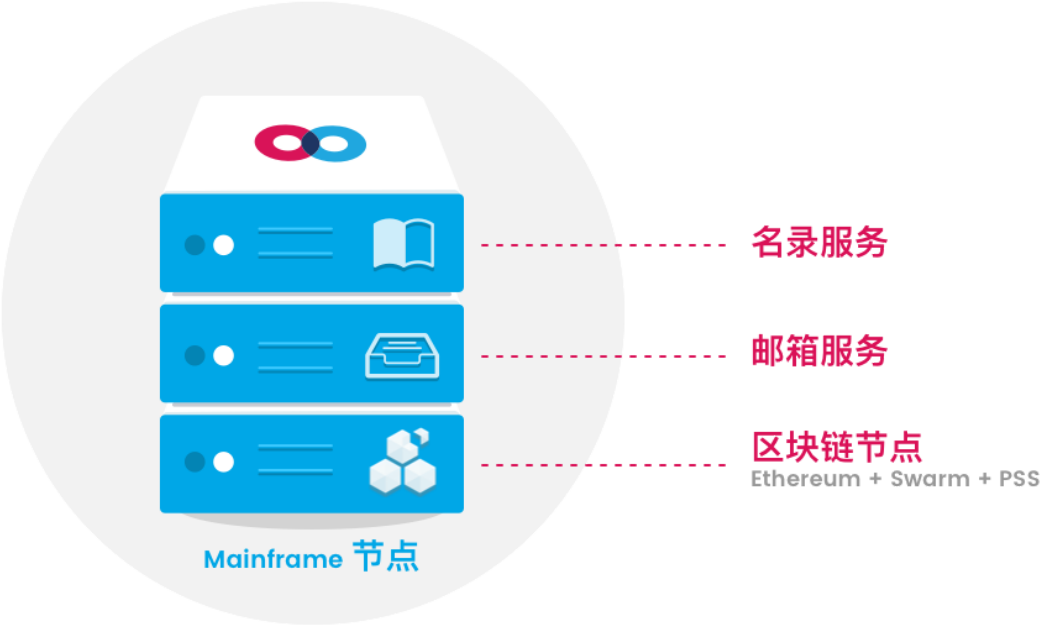
Mainframe平台能被用于社区建设，创造出像推特或Reddit等去中心化的系统。支付系统正迅速增加，但实际生活中，大多数用户应用程序仍然高度中心化，从而受到监管和干扰。Mainframe平台助力许多去中心化、面向用户的金融应用程序，例如微信或Venmo，却又不依赖于任何主机或提供商。

发展路线图

继Mainframe平台与Onyx首次展示后，Mainframe又确立了以下里程碑项目。

里程碑1——“Apollo”

目前并非所有关于完全无主机应用程序的协议都能被使用，因而Mainframe的第一块里程碑将是需要用于过渡期的托管基础架构。该基础架构对每个用户或机构的需求则称为Mainframe节点，它包含一个区块链节点、一个通信层和多项对存储信息和管理合约来说很必需的服务。第一个被Mainframe支持的区块链将是Ethereum，该区块链将使用Swarm分布式存储平台和PSS安全通信协议，实现能抵御监视的封包路由和文档存储服务。Mainframe支持以太坊基金会（Ethereum Foundation）对Swarm的战略观点，并投入重要工程资源，用于改善平台，加速数据传输，促进大众对该平台的接受度。



在这种混合运营模式下，Mainframe最大程度地保障了用户主权。用户可以用Mainframe代币订阅其托管节点服务，还可享受快捷便利，选择自托管方案，部署当前流行的基础架构平台。

Onyx的测试版本即将发布，它能向用户提供：

- 稳定的个人和群组通讯
- 可靠的文件附件，并支持常见MIME类型文件的查
- 全文检索信息和联系人

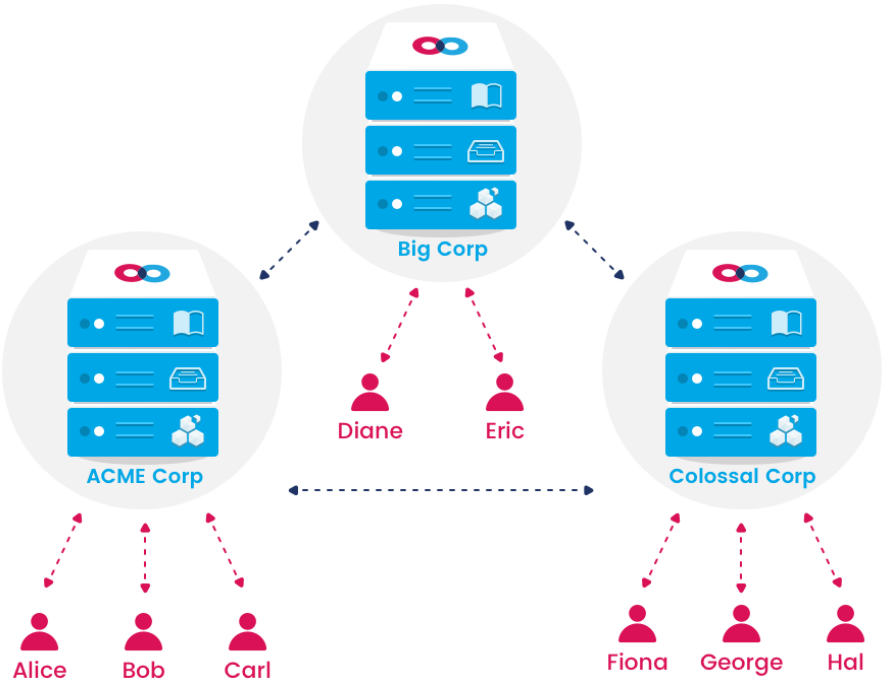
里程碑2——“Hawthorne”

这次发布将从受奖励的封包路由见证激励制的开始，包括节点服务发现、功能性交换合约和发票。

Onyx将继续使用部分混合式的托管基础架构和共享邮箱的运营模式。在默认的最安全运营模式中，每个Mainframe节点只为一名用户提供服务，以确保用户所存储的信息不会被纳入共享数据库。但某些公司所在的行业要求数据保留和数据审核。而在这种运营模式中，企业愿意服从要求，从用户那获取额外却又必要的信任。

在共享邮箱模式中，一个机构内的所有用户共享同一个Mainframe节点。此节点是机构内所有用户发送信息的传输层。一名机构成员会对信息加密，通过Mainframe节点发送出去，而信息在通过传输层时又会被再度加密。当Mainframe节点接收到共享邮箱模式用户传来的信息时，同样的过程会反向发生。这能确保即使在此模式中，唯有私有密钥持有者能看见信息。

然而共享邮箱模式下，信息在被破解后需要更高级别的信任。被破解的信息将以未加密的格式传递、存储至邮箱服务。因此该节点的其他所有用户均能检索和获取此信息。用户权限仍需要认证，用户也只能获取它们自己的信息，但所有信息会被存储至共享数据库。获得正确许可的管理员能审查和查阅此数据库。



共享邮箱模式

Onyx的其他特性也将得到实现，包括：

- 企业级联系人管理
- 线程
- 反应
- 表情
- 备忘录
- 备忘录
- 在线

里程碑3——“Gettysburg”

Mainframe致力于创建一个完全去中心化的通信平台，而这个里程碑将成为Mainframe的巅峰。它将全面支持、激励所有协议层，包括封包路由、数据包发送、包持有、文档存储和数据服务，使Onyx能在完全无主机的模式中运行。

未来Mainframe将推出更加丰富的身份和用户信誉评级API，帮助节点规避违约风险。

此次发布还将包括我们的开发者软件SDK，使个人用户、创业公司和其他机构能在Mainframe平台上开发应用程序。

我们也将发布一个由用户监管的完全去中心化交易市场，令人人都加入其中，体验代币新经济。该市场中的产品和服务全由开发者设计。

最后，这次发布将包含智能合约和预言机，促进Mainframe与其他区块链和发展范式激励层的交互。

尾注

1. Elliott, Francis; Duncan, Gary (2009). *The Times of London*: "Chancellor Alistair Darling on brink of second bailout for banks." https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h

2. Anonymous (2017). *Edelman Insights*: "2017 Edelman TRUST BAROMETER™- Global Results." https://www.slideshare.net/EdelmanInsights/2017-edelman-trust-barometer-global-results-71035413

3. Rogers, Simon (2011). *The Guardian*: "Occupy protests around the world: full list visualised" https://www.theguardian.com/news/datablog/2011/oct/17/occupy-protests-world-list-map

4. Yonego, Joris Toonders (2014). *Wired*: "Data Is the New Oil of the Digital Economy." https://www.wired.com/insights/2014/07/data-new-oil-digital-economy

5. Vanian, Jonathan (2016). *Fortune*: "Why Data Is The New Oil" http://fortune.com/2016/07/11/data-oil-brainstorm-tech

6. Akhtar, Omar (2014). *DMN*: "Why Data is the New Oil" http://www.dmnews.com/marketing-strategy/big-data-is-the-worlds-natural-resource-for-the-next-century--ibm-ceo-ginni-rometty/article/346991

7. Anonymous (2015). *Juniper Research*: "Cybercrime Will Cost Businesses over $2 Trillion by 2019." https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

8. Simmons, Randy (2017). "How Chinese hacking felled telecommunication giant Nortel" https://www.linkedin.com/pulse/how-chinese-hacking-felled-telecommunication-giant-nortel-simmons-1

9. McMillan, Robert; Knutson, Ryan (2017). *The Wall Street Journal*: "Yahoo Triples Estimate of Breached Accounts to 3 Billion." https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804

10. Gara, Tom; Warzel, Charlie (2014). *Buzzfeed*: "A Look Through The Sony Pictures Data Hack: This Is As Bad As It Gets" https://www.buzzfeed.com/tomgara/sony-hack

11. Franceschi-Bicchierai, Lorenzo (2016). *Motherboard*: "How Hackers Broke Into John Podesta and Colin Powell's Gmail Accounts." https://motherboard.vice.com/en_us/article/mg7xjb/how-hackers-broke-into-john-podesta-and-colin-powells-gmail-accounts

12. Lewkowicz, Kayla (2017). "The Top 10 Most Popular Email Clients of 2016." https://litmus.com/blog/the-top-10-most-popular-email-clients-of-2016

13. Galloway, Scott (2017). *L2*: “Lie to Me.” https://www.l2inc.com/daily-insights/no-mercy-no-malice/lie-to-me

14. Andreesen, Mark (2011). *The Wall Street Journal*: “Why Software is Eating the World.” https://a16z.com/2016/08/20/why-software-is-eating-the-world

15. Braden, Robert et al (1989). “Requirements for Internet Hosts -- Communication Layers” https://tools.ietf.org/html/rfc1122

16. Mockapetris, Paul (1987). “Domain Names: Concepts and Facilities.” https://tools.ietf.org/html/rfc1034

17. “Bylaws for the Internet Corporation for Assigned Names and Numbers.” https://www.icann.org/resources/pages/governance/bylaws-en

18. Dierks, Tim; Rescorla, Eric (2008). “The Transport Layer Security (TLS) Protocol Version 1.2.” https://tools.ietf.org/html/rfc5246

19. Russell, Jon (2017). "Cryptocurrency exchange EtherDelta suspends service following alleged hack" https://techcrunch.com/2017/12/20/etherdelta-suspends-service/

20. Postel, Jonathan (1982). “Simple Mail Transfer Protocol.” https://tools.ietf.org/html/rfc821

21. Crispin, Mark, R. (1994). “Internet Message Access Protocol - Version 4” https://tools.ietf.org/html/rfc1730

22. Hansen, Tony et al (2009). “DomainKeys Identified Mail (DKIM) Service Overview.” https://tools.ietf.org/html/rfc5585

23. Oikarinen, Jarkko (1993). “Internet Relay Chat Protocol.” https://tools.ietf.org/html/rfc1459

24. Saint-Andre, Peter (2011). “Extensible Messaging and Presence Protocol (XMPP): Core.” https://tools.ietf.org/html/rfc6120

25. Zimmermann, Philip (1991). “Why I Wrote PGP.” https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

26. Grossman, Lev (2016). TIME: “Inside Apple CEO Tim Cook’s Fight With the FBI.” http://time.com/4262480/tim-cook-apple-fbi-2

27. Ong, Thuy (2017). *The Verge*: “WhatsApp reportedly refused to build a backdoor for the UK government.” https://www.theverge.com/2017/9/20/16338128/whatsapp-reportedly-refused-request-uk-government-access-encrypted-messages

28. Reimer, Jeremy (2008). *Ars Technica*: "Bavarian government caught looking for Skype backdoor." https://arstechnica.com/information-technology/2008/01/bavarian-government-caught-looking-for-skype-backdoor

29. Conrad, Alex (2017). *Forbes*: "Slack Passes 6 Million Daily Users And Opens Up Channels To Multi-Company Use" https://www.forbes.com/sites/alexkonrad/2017/09/12/slack-passes-6-million-daily-users-and-opens-up-channels-to-multi-company-use

30. Shaban, Hamza (2018). *The Washington Post*: "Slack went down, posing a momentary crisis in offices around the country." https://www.washingtonpost.com/news/the-switch/wp/2018/01/09/slack-went-down-posing-a-momentary-crisis-in-offices-around-the-country

31. Maymounkov, Petar; Mazières, David (2002). "Kademlia: A Peer-to-Peer Information System Base on the XOR Metric." https://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf

32. Holbrook, Louis (2017). "Postal Services over Swarm." https://github.com/ethersphere/go-ethereum/blob/ddfc0a2a02ce574f4c252068ce81f0f5ada1c1ff/swarm/pss/README.md

33. Wood, Gavin (2015). "Whisper Wire Specification." https://github.com/ethereum/wiki/blob/965b7cd71fdcf2b8b2de8d36061b0b45678072d2/Whisper-PoC-2-Protocol-Spec.md

34. Trón, Viktor; Fischer, Aron (31 Dec 2017). "Generalized swap, swear, and swindle games." https://www.dropbox.com/s/7r3jasjho35ojc7/sw3paper.pdf

35. Ibid, 19

36. Trón, Viktor; Fischer, Aron; Nagy, Dániel; Felföldi, Zsolt; Johnson, Nick (2016). "Swap, Swear, and Swindle: Incentive System for Swarm." http://swarm-gateways.net/bzz:/theswarm.eth/ethersphere/orange-papers/1/sw%5E3.pdf

37. Anonymous (2017). "Wolk SWARMDB: Decentralized Database Services for Web 3." https://wolk.com/whitepaper/WolkTokenGenerationEvent-20170717.pdf

38. The term "unhosted" and the conceptual diagram have been adapted from remotestorage.io.

39. "Ethereum Name Service." https://ens.domains

40. "uPort: Self-Sovereign Identity." https://www.uport.me

41. "Sovrin: Identity for All" https://sovrin.org

42. Newman, Lily Hay (2016). *WIRED*: "What We Know About Friday's Massive East Coast Internet Outage" https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn