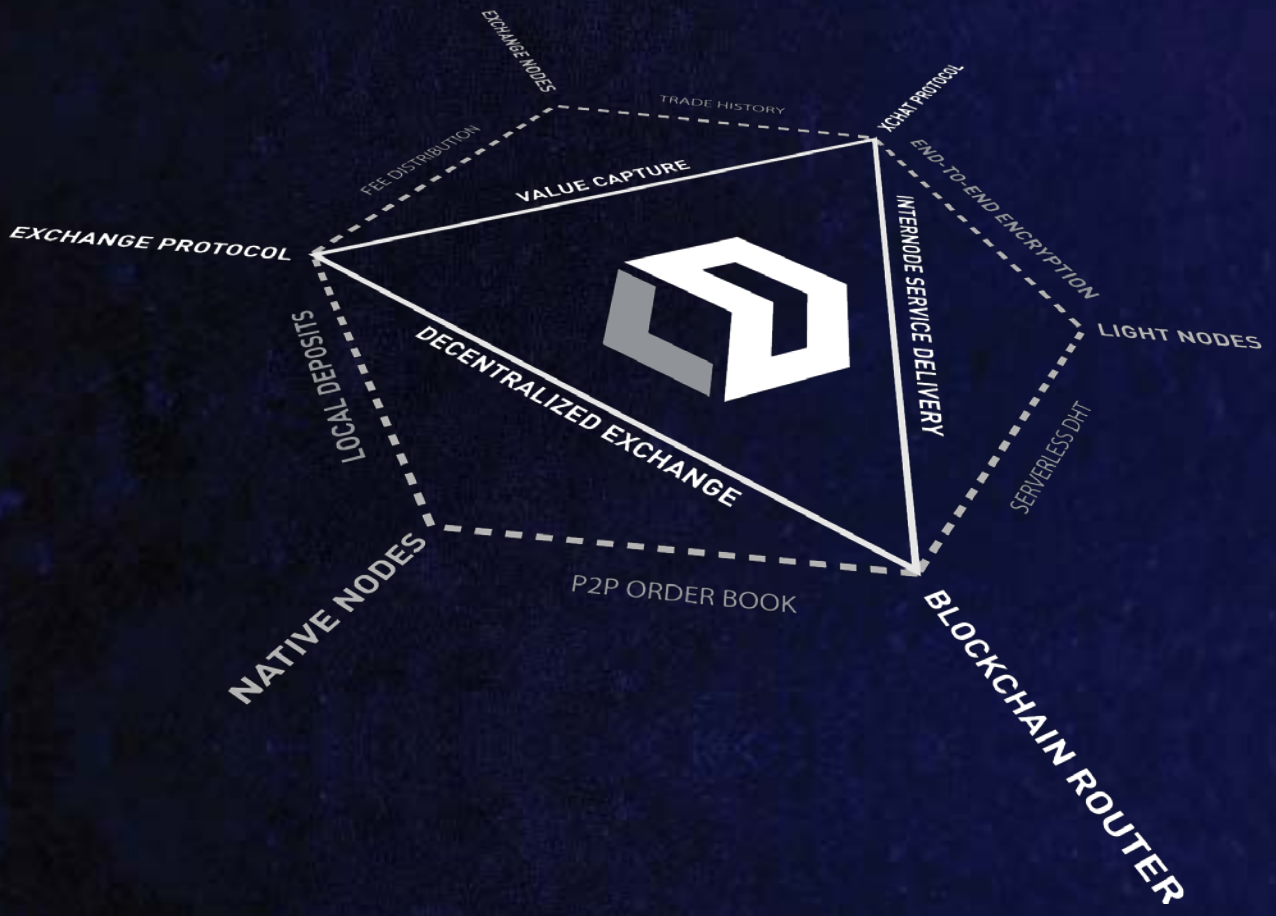


BLOCKNET

设计规格

Arlyn Culwick 和 Dan Metcalf 编写

Alex Koch 和 Blocknet 核心团队做出相应贡献

目录

版本控制

日期	版本号	贡献者	注释
2016-08-27	0.1	Arlyn Culwick	初步的（概念性）草稿
2017-05-18	0.2	Arlyn Culwick	初稿
2017-10-26	0.3	Arlyn Culwick	修改结构以阐明概念
2018-01-20	0.4	Arlyn Culwick	取消低层次的文档内容，改进了关注点
2018-03-07	0.5	Arlyn Culwick	阐述了区块链路由的设计空间；重写和组织有关服务节点的材料。
2018-03-09	0.6	Arlyn Culwick	完成服务节点材料的草稿；完成了订单系统的协议草稿，添加了订单匹配系统部分，起草了订单历史记录的协议草稿。
2018-03-11	0.7	Arlyn Culwick	加入了注册表服务部分；完成了诸多细小的编辑工作。
2018-03-11	0.8	Hanni Abu	审稿并修正了一些印刷错误。
2018-03-12	0.9	Alex Koch	加入若干链间基础设施的使用案例。
2018-03-15	1.0	Arlyn Culwick	最终签署发布第一个公开版本。

引言

本文档旨在面向非技术型的读者和开发者，前提是此类读者对区块链的定义至少有总体的了解。Blocknet 设计和架构的引入在很大程度上是非技术性的，期间不仅借助了图表，还通过逐步的方式说明链间服务的定义以及链间基础设施服务最低限度必须提供的功能。随着文档更新频率的增加，讨论的内容也从链间服务的定义等方面转变到 Blocknet 的具体规格。通过将设计方面与实施和集成相结合，预期的结果是我们开始探讨 Blocknet 的系统设计规格。

我们发布此文档的原因

我们相信，设计解决方案的最佳方式无疑是进行广泛的沟通并获得对我们工作的多角度见解。我们也相信，通过公开我们的工作，我们可以让广泛的人员参与到项目和代码编写工作中并借此获益。此外，在基础设施项目中，让使用和利用我们技术的人员参与其中是非常重要的举措。

有些人可能担心竞争对手会抄袭我们的工作并获得竞争优势，特别是因为我们的设计不仅是首次推向市场，也尚未取得重大突破。尽管如此，我们仍然迫切希望得到加密和企业架构社区的综合性见解，因此风险回报率让我们毫无顾虑。

欢迎贡献者

Blocknet 既不是公司，也不是专属团队，而是专门的基础设施，并且我们相信基础设施应该是公有的，可以免费提供给所有人。

此文档目前只是草稿，而不是最终的设计。事实上，最终设计的概念在实践持续发展的项目中没有明确的定位。我们欢迎对本文档的内容做出贡献和参与讨论。

Blocknet 的代码是开源的，任何人都可以为 Blocknet 项目做出贡献。

当各种观点和技能对项目的设计和实施产生影响时，类似于此的项目将得到最大的受益。我们欢迎各方面的合作。

若要对 Blocknet 做出贡献，请发送电子邮件至 contact@blocknet.co。

发展机遇

Blocknet 简介

Blocknet 是面向即将到来的“区块链间时代”的基础设施，这是一个新兴的技术时代，主要表现为当前的 API 生态系统取代了分散和本质货币化的“令牌生态系统”。当其支持技术（特别是智能合约和“分布式应用程序”）成熟到具备实用的区块链间互操作性时，就会出现这种转变。在编写本文时，Blocknet 是提供分布式应用程序和智能合约所使用之链间基础设施的技术领先者。

我们认为，区块链间时代的兴起将对两个行业产生颠覆性影响，即软件即服务和实用区块链的可用性。

从软件即服务 (SaaS) 的角度来看，令牌生态系统体现了两方面的基本进步：(a) 数字服务的相对无阻力货币化，以及 (b) 充分利用区块链技术独特的稳健性、分散性和安全性。

从区块链技术的角度来看，如果区块链要充分发挥其真正的潜力，那么区块链服务之间需要实现广泛的通用互操作性。如果没有链间的互操作性，基于区块链的服务将 (a) 仅在运行其节点的有限客户群范围内提供服务，或者牺牲区块链在交付给集中实体时具备的独有安全性，以及 (b) 面临持续的链膨胀问题，与此相对应的是，与市场有关的压力将更多的功能集成到单一链中。

通过创建“区块链互联网”，Blocknet 定位为实现 API 的无阻力货币化，并通过将其数千个独立的链转化为令牌生态系统来增强区块链技术。

痛点

基于互联网的传统服务在其技术栈中面临着长期的不安全性。此外，它们通常需要集中功能和数据，给客户带来高度的信任负担。相比之下，借助区块链技术，人们能够利用加密的证据来提供“不可靠”的服务，其中每个参与实体均可以证明自己对给定结果的确定性，从而在根本上降低与另一方开展业务时所需的信任程度。这就系统地扩大了经营方式的范围，实现了许多新的业务模式，并且可以提供明确定义的安全保证，降低成本并更好地保护品牌价值。

然而，区块链不能立即展现其真正的潜力，主要原因在于它们不可实现互操作。当前有数千个区块链，但它们发挥的功能类似于与互联网断开连接的局域网，并且尚未营造出能够推动通用互联带来之划时代变革的环境 – 这种变革的规模应类似于互联网推动 Facebook 和谷歌等大型网络公司的涌现。

解决方案

Blocknet 是令牌生态系统的基础设施。它在不同区块链上的节点之间提供真正的对等互操作性，以便实现以下功能：

- 将*任何*类型的数字服务从任何区块链上的一个节点提供给另一个节点。
- 任意给定区块链服务的功能均非充当“应用币”，而是作为“协议服务”，也就是说，任意区块链上的*任何其他*分布式应用都可以出于开放目的而予以使用，而不仅仅是作为其创建者的分布式应用，这就有效地扩大了服务的市场覆盖面和收入来源。
- 智能合同令牌的功能不仅仅是为了货币化分布式应用，而是要成为“协议令牌”，这就从逻辑上将其置于技术栈的较底层，其潜在效用更大。此外，服务的代码质量可能会受益于来自不同社区的广泛开发者基础，充分利用他们的综合学习知识，防止链膨胀和代码重复，节省劳动力时间，并为*整个*区块链消费市场提供服务，而不是只服务其区块链的一组用户。
- 分布式应用能够简单地编排链间服务，而不是从头开始编写复杂的代码。因此，主要的开发任务就成为 API 集成，而不是编写全新“防弹”智能合同这一复杂而高度专业化的任务。
- 借助微服务架构构建分布式应用，其中每个区块链均可提供单一服务，并以模块化方式与许多其他服务集成，带来更简单的组件设计、更轻松的错误修复以及更简便的升级。
- 能够有效地绕过选择区块链构建基础的（当前困难的）问题 – 不仅是在项目启动时，还在其生命周期的后期阶段，以及各种微服务可能更好地在不同区块链上实施时。
- 利用其内在的令牌价值实现链间和多链式服务的货币化。
- 充分利用区块链技术带来的全新加密经济型商业模式。例如，企业可以直接根据货币政策（ICO、交易费用、通缩经济、区块奖励和超级区块自筹资金系统）以及货币化 API 的市场，从“优于免费”的模式中提取价值。

Blocknet 应通过基于架构和协议的方法来实现上述目标，相关文档就是本文的主题。

设计

设计目标

以下特性应按照优先级的降序设计：

1. 互操作性

首先，Blocknet 是区块链间的基础设施。因此，其最直接的设计目标应该是与绝大多数现有和未来区块链实施之间实现互操作性。此外，它应与集中式实体互操作，以便在令牌生态系统中提供基于服务器的传统服务。

2. 分散性

实质上，分散性就是指没有一个实体能够对系统中的其他实体进行控制。例如，比特币的主要成就在广义上就是货币的分散性，其中没有一个实体进行控制。

(a) 货币价值、(b) 资金转移、(c) 保存记账记录和 (d) 货币政策。

然而，比特币目前存在于很大程度上集中的生态系统中，因此在实践中取消了它的许多优点。由于 (a) 已经以 API 生态系统的形式存在，并且 (b) 感兴趣的特性（即分散性）在服务交付期间很大程度上会丢失，因此提供分散式服务交付的集中生态系统几乎没有价值。例如，如果有人使用集中交易所购买比特币，此购买并非“不可靠”，因为人们必须信任交易所，并且购买受到传统支付基础设施的所有常见影响（银行费用和延迟、支付网关费用、签证和万事达卡费用、欺诈风险、KYC 要求、借助金钱和个人信息信任许多中间商的要求等）。因此，为了使比特币和其他各种分散技术充分返回其潜力，需要建立一个分散的生态系统，其中实体可以在不影响技术变革力的情况下开展业务。

3. 安全性

分散化和货币化服务的特点是要求在与航空应用相当的水平上具有高度的安全性和运营确定性，因为 (a) 通常不可能改变在其网络边缘运行的服务或使其下线，(b) 如果发现资金在不受集中整顿的系统中可能被盗用，那么它很快就会失去大部分的价值。出于这些原因，Blocknet 需要最高级别的安全性和运营确定性。

4. 无需信任的服务交付

在区块链的背景下，分散性带来的频繁且令人满意的结果是，不一定要确信交易对方在交易过程中诚实行事。例如，对于比特币，人们无需信任中间商转账资金或收款人诚实地报告是否收到付款或其金额是多少，因为不涉及中间商，交易对方可以极具信心地独立验证付款状态。

在链间服务交付的情况下，于区块链之间进行服务支付时需要相同程度的“非信任性”，以便可以在不要求参与者诚实行事的情况下提供和支付服务，从而在链间环境中保持区块链支付的这一独有特性。

5. 简单集成（无需编写代码）

为了最大限度地提高互操作性并减少阻力，Blocknet 的集成和令牌生态系统的访问不需要修改库存钱包或节点。请注意，使用通过 Blocknet 进行交付的某些第三方服务可能需要编码，但使用 Blocknet 本身不需要编写代码。

6. 分散集成

为了最大限度地提高安全性并建立一个开放的、互联网式的生态系统，Blocknet 的集成和令牌生态系统的访问不需要任何中央实体（甚至是我们）的调解。要通过 Blocknet 交付或使用服务，消费者不应被要求 (a) 使用 Blocknet 的区块链、(b) 使用任何特定服务或 (c) 使用任何具有集中效应的服务（这里的“集中”用来表示一系列情景，从中央代理的控制到其网络周围其他网络的侧链式集中，后者我们称之为“链间集中”）。

请注意，使用通过 Blocknet 交付的某些第三方服务可能需要某些中央方的调解，但使用 Blocknet 本身不需要。

7. 可组合性

Blocknet 的构建应尽可能考虑到可组合性和模块性，与上面设想的链间微服务的模式相同。具体来说，微服务设计的关键原则是最大限度地提升可组合性，同时注意哪些服务总是同时使用，以避免构建“分散式整体”。这些服务在令牌生态系统中保持不变。

8. 货币化

在令牌生态系统中，可组合性原则加入了一条关键原则：服务在本质上可以货币化。如果不可货币化，那么我们建议将其捆绑到可货币化服务的 API 中，否则运行服务节点的人员可能会缺乏相应理由，因为他们无法从中获得收益。

此外，服务的收入来源需要通过一些无需信任度的协议或加密经济激励措施来*保证安全*，否则不太可能实现其价值。货币化是这样一类问题：您的服务消费者是否愿意为此付费，因为这是他们是否无法强行免费使用此服务的问题。

Blocknet 应在可行的情况下对其核心服务进行货币化，免费提供其他服务，并应提供各种方式，让通过 Blocknet 交付的服务可以借此安全地货币化。

9. 移动性和小足迹性

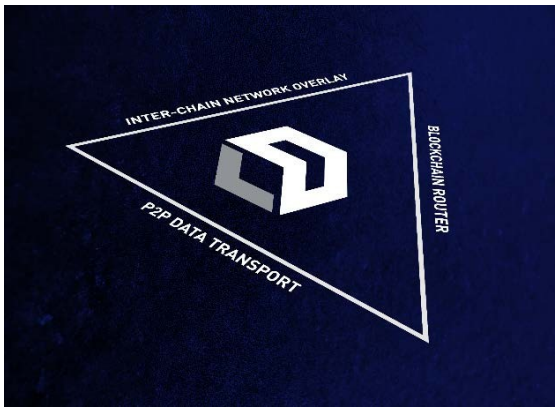
在保险、健康、供应链、农业、汽车远程信息处理和安全行业中，从移动应用到嵌入式物联网设备的多种场景都支持令牌生态系统。[1] 我们预计将会涌现的许多使用案例均需要足迹非常小的分布式应用，而此类应用无法托管甚至是单个区块链。Blocknet 应为这些设备提供对令牌生态系统的访问权限，以便它们可以利用区块链特有的安全性，我们认为这对于减少物联网服务的攻击面至关重要。

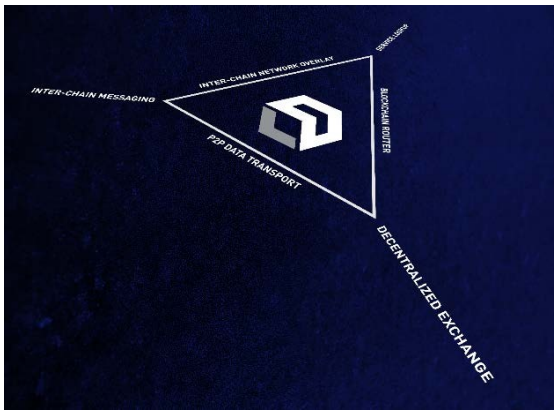
[1] 有关详细信息，请参阅 2015 年 2 月发布的 Blocknet 业务概述。还可通过 contact@blocknet.co 请求提供此业务概述。

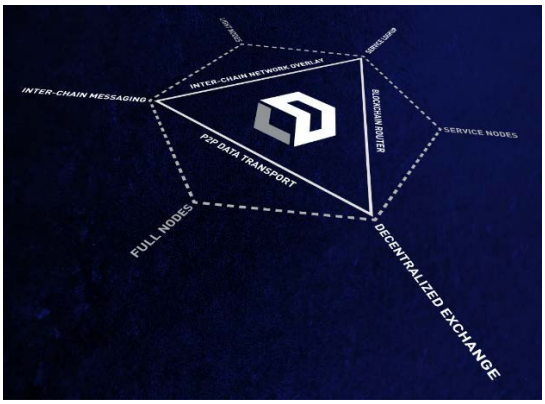
架构

通用区块间互操作性是通过集成三个**核心组件**实现的，这三个核心组件一起提供三项**核心服务**，并伴随着任意数量的**区块链服务**和**区块链组件**。这些服务和组件可支持构建无限数量的区块链间服务 - 令牌生态系统 – 且所有这些都可以编排成**链间应用**。

为了在这个新颖的领域帮助读者，我们通过一系列阐明了组件和服务之间关系的图介绍相关概念。这些图的推进顺序如下：







应首先介绍组件，然后介绍服务。在此之前，应介绍链间架构的一般特性。

链间架构的外观

一般来说，区块链间架构总是会涉及至少两个区块链网络，以及一些额外的实体或功能，用来提供网络之间的互操作性。由于区块链网络是分散和分布式的，因此互操作性组件不应置于某个中心位置；为了保持分散性，它们需要在每个网络边缘的节点上运行或在本地与其交互。

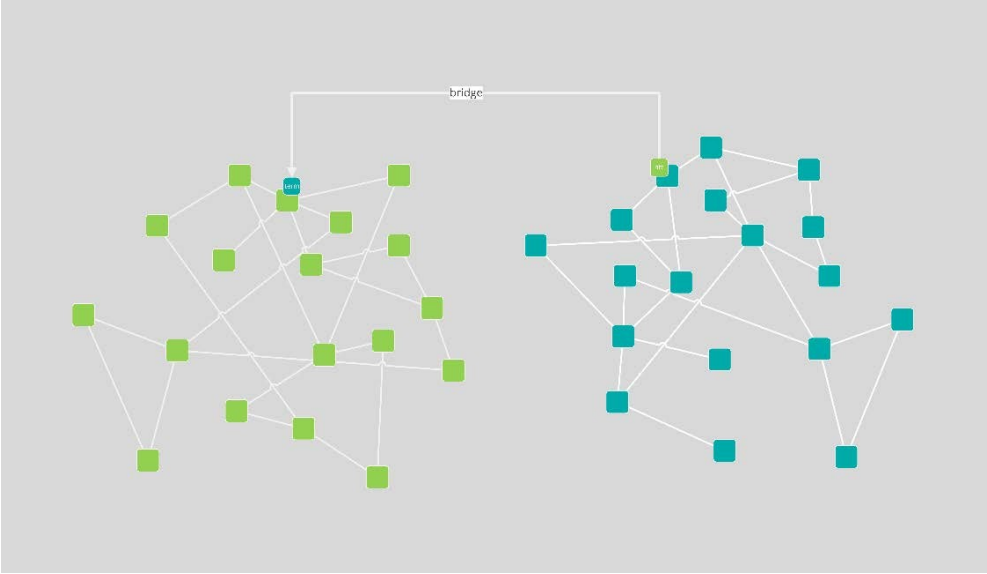


图 1

理想化的一对 p2p 网络，以及从一个节点到另一个节点的中断交付服务。

我们为各种项目提出了以下几种解决方案：

- **传统技术**：集中式中介（例如 Poloniex.com）
- **最大主义者**：一个分散的*网络*，其充当逻辑上集中的中介（例如在侧链环境中的比特币）
- **专有代码**（即钱包、智能合同或钱包附加物），其*仅*在运行此代码的节点（即 BTCrelay）之间实现区块链互操作性。
- **围墙花园**：仅在某些自定义区块链的实例之间存在的链间协议，其使得开发者仅能以此协议进行构建（例如 Aion）。

上述各种链间技术都不是*通用*的，也不是*分散*的。也就是说，它们要么没有为开放式的各种服务（包括*现有*区块链上的服务）提供支持，或者在没有集中控制的情况下无法提供此类支持，从而背离给定的服务对分散的依赖。

根据 Blocknet 的**设计目标**，一个令人满意的解决方案必须是通用的和分散的。我们通过“第一原则”来解决这个问题，也就是说，通过始终忠实于链间场景本身的性质。

1. 分布式网络架构

首先，需要明确的重要事项是，任何链间组件都必须存在于它们与之互操作的网络之边缘。这会将服务分布到每个交付或使用服务的区块链网络。此外，链间组件还必须从自己的网络边缘提供服务，而不需要集中操作，否则它将作为另一个集中式中介。

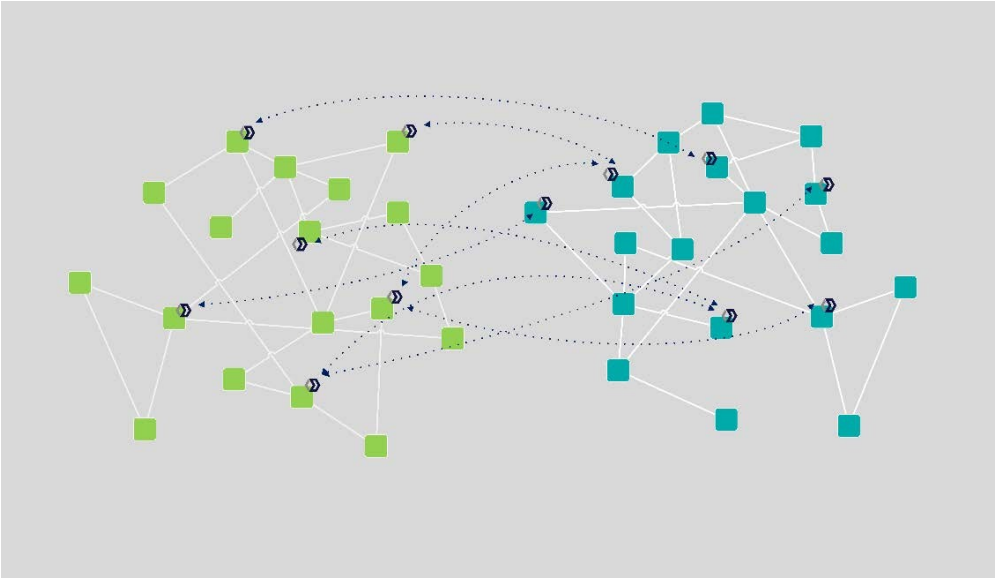


图 2
一个合适的链间服务必须存在于其网络和使用它的网络之边缘。

2. 分散的行为主体

其次（且具有相关性），交付或使用链间服务的行为必须是自主的，即不受第三方控制。从架构上讲（即除协议设计外），实现此目的的最直接和最安全方法是链间服务组件的节点以及使用或交付（或两者）该服务的网络*存在于同一台本地计算机上*。这一要求的严格程度 – 及其影响链间服务足迹的程度 – 会有所变化，从要求运行完整节点到运行 SPV 节点，再到仅仅是签署交易，而最低限度是在低安全性应用程序中查询区块链浏览器网站或其他集中式 Oracle。最后一种程度被视为“链间”一词适用性的限制情况。

因此，全方位的本地架构要求是显而易见的。在除限制情况以外的每一种情况下，每个行为主体都需要以分散的方式参与交付和使用网络。这可以通过遍历上图来以图形方式表示：

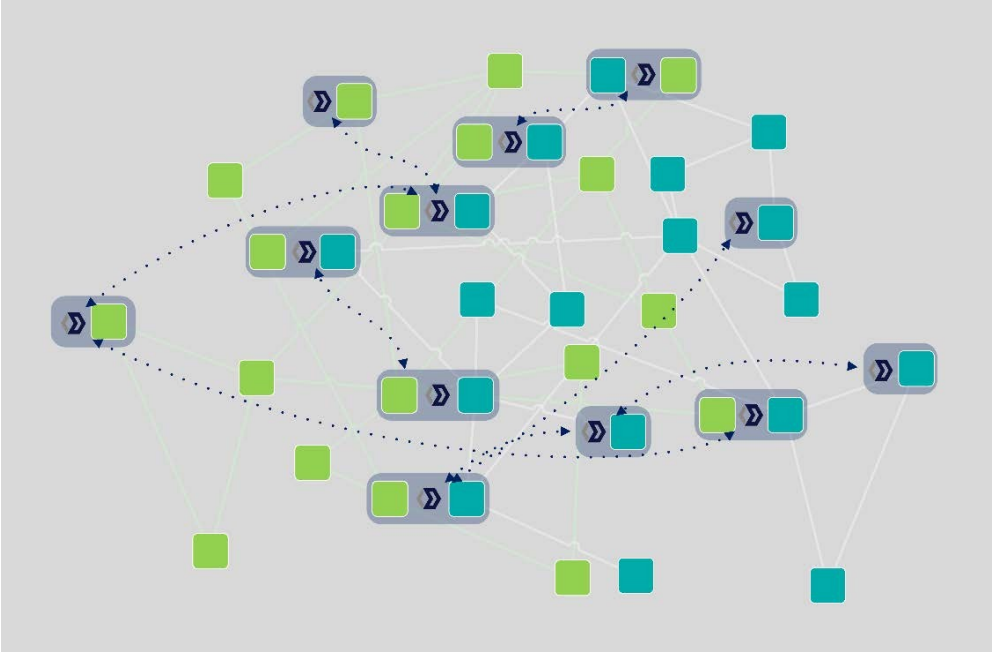


图 3
分散式链间基础设施

蓝色区域表示使用、交付和链式节点的不同组合（蓝色区域外的节点不支持链间服务）。

3. 非区块链锁定

虽然每个链间服务都必须从某些链上的节点提供，但链间基础设施不得限制给定服务可能运行*哪个*区块链，否则所有这一切实质上都是一种分布式客户端-服务器模型，而这实际上是当今集中式应用程序的默认架构。例如，Blockstream 的侧链实施需要每个用户与比特币区块链进行交互，以便消使用任何其他链的服务。我们称这种陷阱为“链间集中”。为了避免这种情况，一个真正的区块链互联网 - 以及一个可以支持令牌生态系统的区块链 - 必须能够通过区块链交付或使用服务。

这种链不可知的概念激发了集成需求和应用足迹的谨慎最小化。例如，如果 Blocknet 要求链间服务的每个消费者保留 Blocknet 区块链的副本（除了服务提供商的区块链之外），那么它的用处将是相当有限的，并且用户阻力会非常大。

链间基础设施设计的这一方面将主要承担服务的货币化交付，原因有两点：第一，在点对点网络中，行动主体不可信，并且支付和服务交付必须是原子的。其次，节点必须由具有不同本地令牌的节点在其本地令牌中支付，因此它们必须交换，而分散交换需要高度的安全性和代码质量。但是，如果需要下载和维护两个甚至三个区块链以便使用该服务，则它不太可能会被广泛采用。因此，Blocknet 应提供避免这种情况的方法。

总结

上述考虑事项为 Blocknet 组件的设计提供了三个指导原则：

1. 链间基础设施服务必须在*其*网络以及任何服务交付和使用网络的边缘运行。
2. 从架构上讲，通过在同一台本地计算机上运行交付或使用服务所需的组件，最容易实现服务分散。
3. 链间基础设施服务必须尽可能限制其集成需求和足迹。

核心组件

Blocknet 包含三个核心组件，它们共同充当通用链间服务基础设施的基础：

- **XBridge**，链间网络覆盖层
- **XName**，区块链路由
- **XChat**，p2p 数据传输

这三个组件定义为“核心组件”，因为从直观上来说，任何链间互操作性解决方案都必然需要不同底层网络上节点之间的一些联网方法，通过这些方法，节点可以发现将服务请求路由到何处；以及一旦找到合适的节点，还需要用于 p2p 通信的一些协议。

为了帮助读者记住和展现 Blocknet 中的组件和服务的复杂性，我们随着元素的引入逐渐构建图形。下图仅显示了 Blocknet 的三个核心组件。

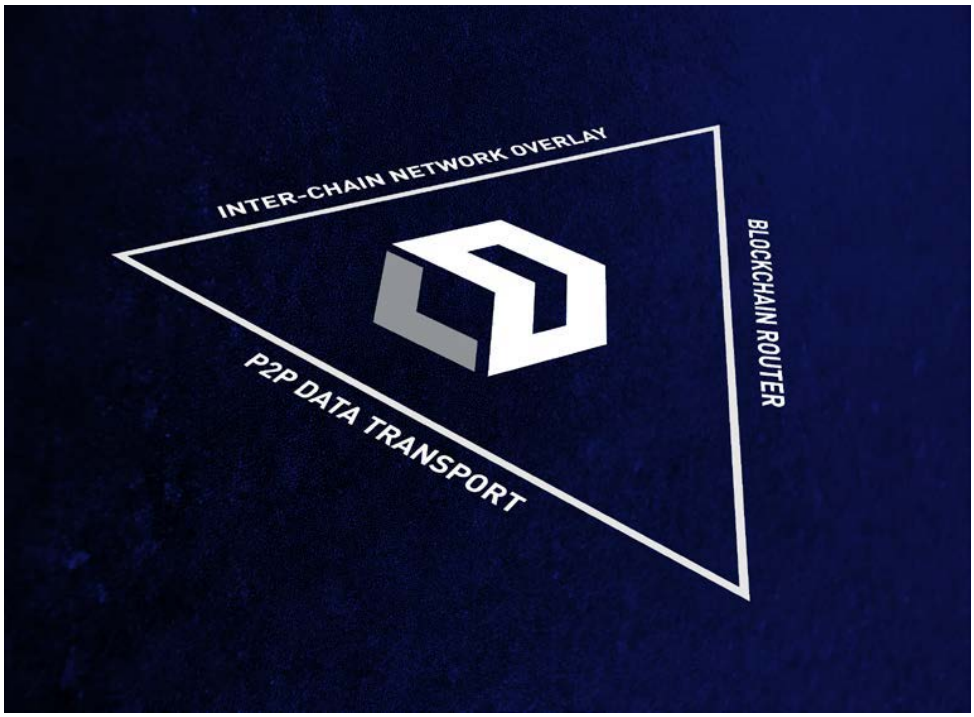


图 4
第一次迭代：Blocknet 的三个核心组件。
一个三角形若要存在，必须有三条边通过它们的顶点连接，这表明了这些组件对于提供链间服务的共同必要性。.

XBRIDGE：链间网络覆盖层

Blocknet 采用了 XBridge，这是一种无服务器的、基于 DHT 的点对点网络。在给定的本地机器上，此网络上的节点与*其他*网络上的节点集成在一起，从而使我们的网络成为链间网络覆盖层。这就实现了任何区块链网络上节点之间的查询、定位和不昂高。

上下文图

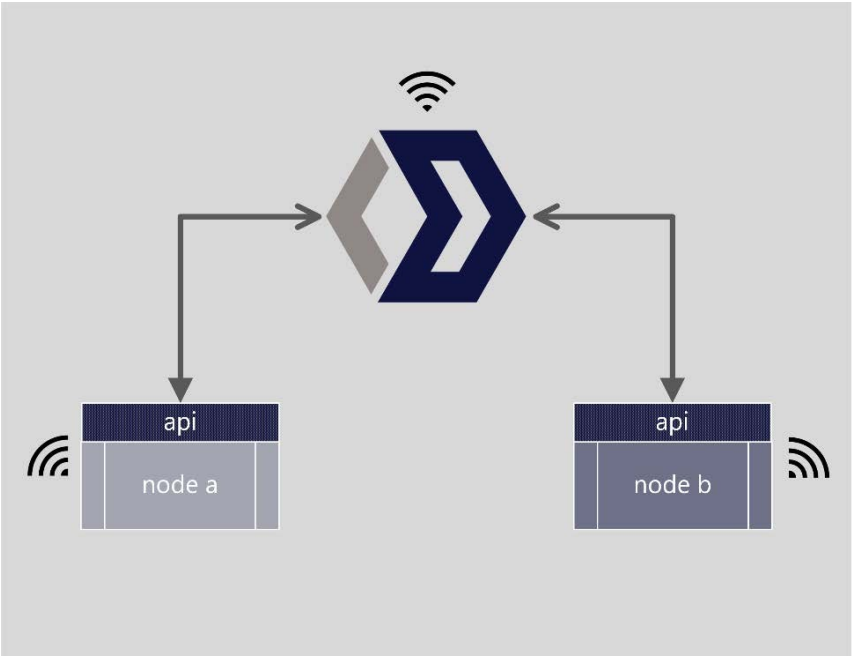


图 5
本地机器上的网络组件

有关技术文档，请参阅**技术规格**一节。

具体实施

目前：网络覆盖层代码在 Xbridgep2p.exe 和 Blocknet 钱包中实施。其未货币化。

未来：此覆盖层可能会在代码库中模块化，但它不太可能作为独立应用发布，因为其将与其他组件交互以提供**核心服务**。

XNAME：区块链路由

链间服务的生态系统需要一种将消息路由到正确区块链的方法，而在 Blocknet 中，应通过链间地址系统来实现这种路由。区块链路由处于初级设计阶段，需要更广泛的加密社区进行探索和协商，但从根本上讲，它需要通过链间标准来指定区块链，如 Uport 的 MNID，以及指定将路由数据提交到注册表的方式和查找功能。一个有待解决的关键问题是路由结果的最优价格与真实性之比。例如，服务可能从免费注册表服务中受益最多，并且通过在付款和交付之前消除查找后得到不真实结果的可能性，其可接受一定程度的不良查找结果。或者，某些服务可能需要可靠的查询结果，并且可接受由此产生的少量费用。XName 应对注册表服务设计采取不可知的方法，其应在必要时提供成熟的解决方案以满足各种集成商的需求 - 包括出现竞争激烈的注册表服务市场的可能性。

因此，逻辑路由器的设计方向是缓解 (a) 查找的真实性和成本问题以及 (b) 将路由数据提交给专用注册表服务的相关问题 - 包括查找注册表服务的链 ID。由此，XName 的功能就是调用注册表服务的 API，并且在完成服务交付后本地存储路由结果的缓存。

为了在首次启动时改善循环性（也就是在查询服务之前查找注册表服务），节点也可以自行启动并 (a) 查询硬编码的链 ID 以获得可信的真实注册表服务，或者 (b) 通过专用的 getRegistryService 调用查询其在 Bridge 上的对等实体，然后查询返回的每个注册表服务，从而利用每个服务可能提供的真实性保证，以便构建真实的本地注册表服务（和其他链间服务）列表。若要了解如何提交和查找链间服务的问题，请参阅**服务查找**和**注册表服务**部分。

有关技术文档，请参阅**技术规格**一节。

具体实施

目前：区块链路由与其他核心服务一起在 Xbridgep2p.exe 和 Blocknet 钱包中予以实施。

未来：该组件可能总是与其他组件交互以提供**核心服务**，因此不一定会独立部署。然而，可以逐步实现区块链路由的货币化，这可能是因为货币化可以使服务反映其自身的运行成本，允许路由服务之间实现竞争，并且激励服务的技术进步。如果实现货币化，则路由组件可能会额外与其他组件在其自身的区块链网络上集成。

XCHAT：对等数据传输

数字服务的交付需要一种发送/接收消息和服务有效载荷自身的方法。因此，Blocknet 采用了 XChat，这是一种端到端加密的对等消息模块，支持一对一消息和群组消息（广播消息已经通过 **XBridge：链间网络覆盖层**得到支持）。

通信和数字服务交付的要求因服务的性质而异。隐私、带宽、延迟、持久性以及中介商的缺席或存在都是变数。因此，这项服务可能会发展为几种数据传输技术。尽管如此，在这一非常早期的阶段，极其私人、快速、点对点的解决方案似乎已经足够。

可在**技术规格**一节中获得相关技术文档。

具体实施

目前： 数据传输与其他核心服务一起在 Xbridgep2p.exe 和 Blocknet 钱包中予以实施。

未来：此服务可以在代码库中模块化，并且如果它作为独立应用程序货币化，则可能因此发布。

核心服务

货币化的链间服务需要三项核心基础设施服务：

- **服务查找：**一种发现对等体以交付或使用服务的方式
- **链间消息传输：**交付数字服务的方式
- **分散交换：**一种货币化服务交付的方式

这些服务是**核心组件**的*编排*，因此可以在上图三角形的顶点上表示，如下所示：

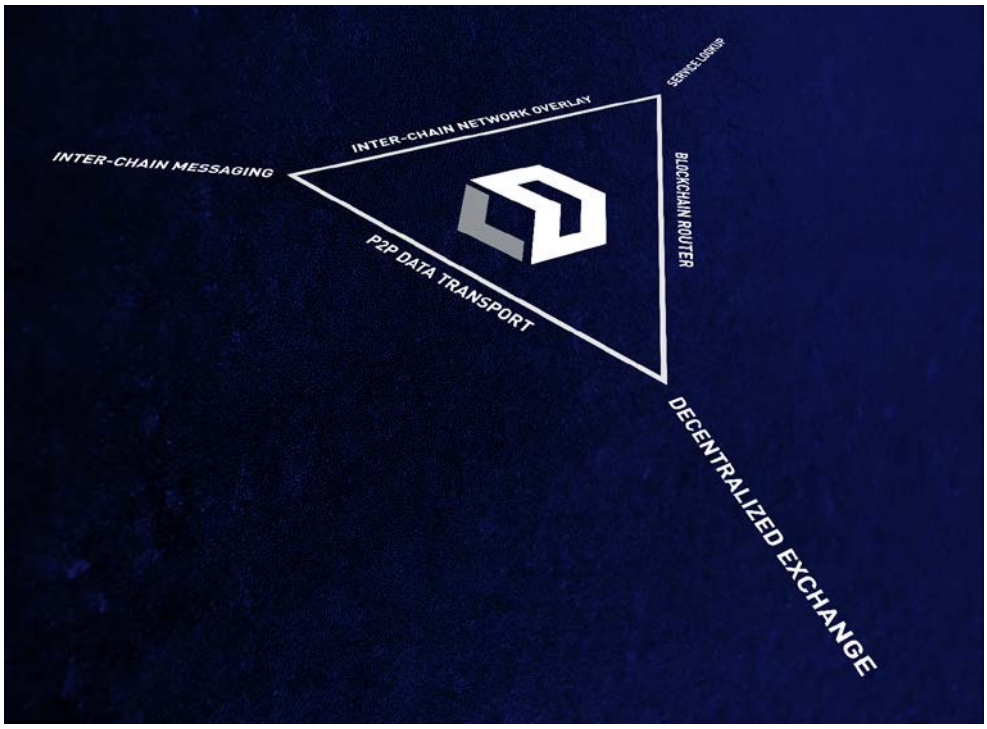


图 5
第二次迭代：
Blocknet 的三个核心服务和组件。
由于三角形的顶点是各服务所在边聚集在一起的地方，因此将服务定位在此可用来表示它们的本质，即核心组件的编排。

服务查找

链间服务查找是 XBridge、XName 和 XChat 组件的编排，并调用 Blocknet 上任意给定的**链间服务注册表**。随着 Blocknet 的不断成熟，其可能抽象为 API 外观。

与传统的互联网一样，各方需要查找并定位彼此以便进行互操作。因此，需要模拟域名系统 (DNS)。但与传统互联网不同的是，服务通常由网络上的任何节点进行对等提供，而不是从可通过单个 IP 地址寻址的服务器提供，因此为了请求服务，其只需要定位给定区块链网络上的*任何*节点。由此，“链式代码”是主要要求，还需要具备其他次要的特性。

假设服务通常应仅*提供*给特定的节点。

注册表服务在非信任节点的对等网络上的一个重要特征是，不同于服务提供商可以合理得到信任的情况，有意图（恶意或其他企图）的*任何人*都可以提供服务。

根据设计策略，无法保证服务查找所返回数据的真实性，因此必须在后期阶段提供服务完整性的保证，或者无论提供服务之节点的意图如何，服务查找必须以加密方式进行以保证数据的真实性。Blocknet 的设计旨在对注册表设计采用的方法提供不可知性。

消息传递步骤

根据前一种设计假设，服务查找的典型步骤是：

1. 在 XBridge 上寻找对等实体
2. 通过 XName 检索服务的链 ID 和服务列表
3. 查询 XBridge 上的对等实体，以在由链 ID 指定的链上找到对等实体
4. 切换到 XChat；获取特定对等实体支持的服务列表
5. 请求服务（并继续构建服务真实性的证明）

根据后一种设计假设，通过采用区块链一致性算法（例如工作证明）可以简单地完成服务查找（即没有来自该项目的原始贡献），并且查找服务的节点在本地托管包含链 ID 数据的区块链，同时免费查询。但是这给用户带来了显著的存储空间和正常运行时间负担，因此预计不会成为使用 Blocknet 的典型方式。在用户维护服务注册表区块链的环境之外，可以使用原始比特币白皮书中所述的 SPV 节点。为了实现更出色的可扩展性和更小范围的应用程序足迹，截至撰写本文时，我们都一直在探索替代的证明系统。有关设计模式，请参阅**交易历史**和**注册表服务**部分。

上下文图

上述步骤暗含了如下的高层次架构：

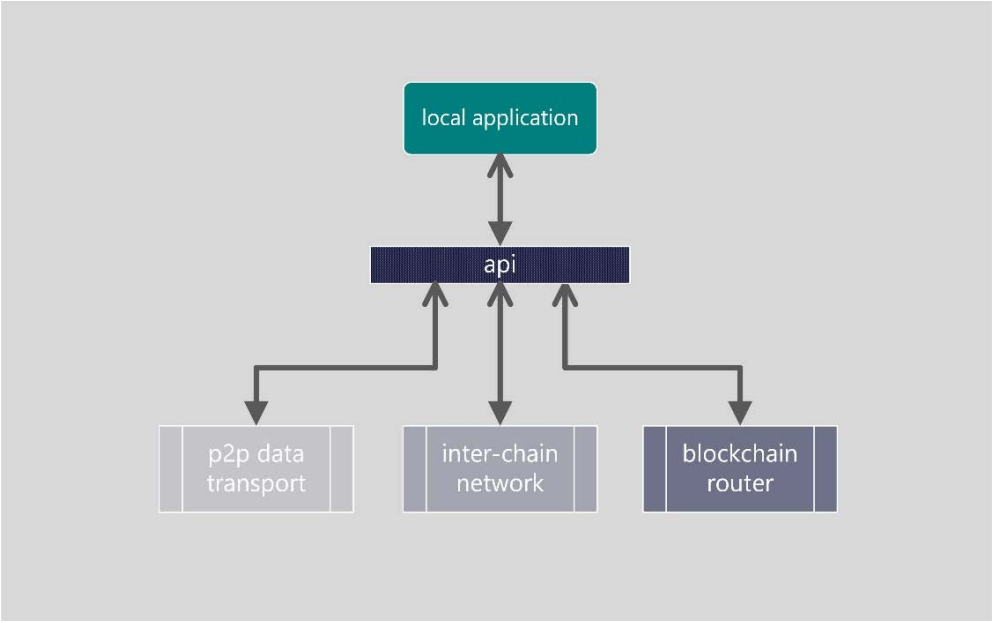


图 6
上下文图表明了本地机器上使用服务查找的核心组件之间的关系。

技术规格一节中提供了相关技术文档。

具体实施

目前：服务查找目前作为 XBridgep2p.exe 的一部分实施或嵌入到 Blocknet 钱包中。在 Blocknet 目前的开发阶段，唯一实施的应用是分散交换，它只需要节点按照货币对进行过滤。因此，更通用的查找服务仍有待建立。

未来：经过适当的探索和区块链生态系统达成的共识，计划开发通用查找服务。此外，为了简化消费者与底层组件的集成，服务查找可能体现在 API 外观中。无论这是所有核心服务的单一外观，还是专门用于查找的独特外观，都可能是满足时间、成熟度和消费者需求的功能。

链间消息传递

链间消息传递是 **XBridge** 和 **XChat** 的编排，并且涉及服务提供商和消费者相互定位、通信和交付服务。

该服务是在假设消费者应主动寻找服务、而服务提供商应被动定位的前提下指定的。

在公共对等网络中，不能认为每个作为服务提供商或消费者的实体都会诚实地行事，因此对于大多数服务而言，有必要在付款前证明该服务的有效载荷是合法的，并且消费者在没有付款的情况下也不能获得服务。换句话说，服务必须既*无需信任*又*自动*地运作。

在这方面实现“无需信任”的有计划方式是使用零知识证明系统。以下是关于 BIP-0199 声明的注释：“存在[各]种实际的零知识证明系统，这些系统用于保证哈希前象衍生出极具价值的信息。作为一个例子，零知识证明可以用来证明一个哈希前象充当加密数独谜题解决方案的解密密钥（请参阅数独支付以了解此类协议的具体示例）”。请注意，为了清楚起见，简单的数字签名方案旨在证明服务提供商实际上是消费者所认为的零知识证明组成部分，就是说服务提供商的私钥没有被透露，而消费者可以证明服务提供商的身份。在一项服务或另一项服务上实施的实际证明方案可能会随着“可靠”交付服务需要证明的事项细节而变化。

此上下文中的原子性是通过下一节介绍的**分散交换**实现的。

消息传递步骤

链间消息传递服务中的典型步骤是：

1. 根据前一节所述，在网络覆盖层上查找服务并请求服务

2. 通过 XChat，服务提供商为证明有效载荷合法性的零知识证明提供材料 - 也就是说，创建一个足以确保有效载荷合法性的一组断言证明（关于基本示例，请参阅**交易历史**一节）
3. 消费者接受此服务
4. 服务提供商继续进行分散交换服务，开始交付服务

为了尽量减少应用程序的组件或简化使用，链间消息传递可能需要独特的 API 外观。这种看似恰当的使用案例服务是免费的，其中链查找可以进行硬编码，例如分散式聊天应用。

上下文图

上述步骤暗含了如下高层次架构：

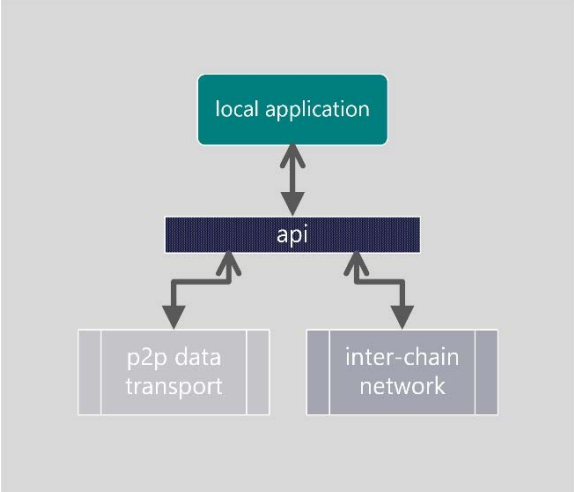


图 7
上下文图表明了本地机器上使用链间消息传递服务的核心组件的关系。.

具体实施

目前：开发人员可能 (a) 将 **XChat** 嵌入他们的应用程序中，以及 (b) 利用网络覆盖层，无论是通过 XBridge 独立应用程序还是 Blocknet 钱包中的嵌入式形式。

未来：组件应模块化并编写 API，此外，可能还有一个 API 外观将两个组件抽象和编排成明确定义的服务。

分散交换

分散交换是一种无需信任的、原子的交换货币方式*或*其他货币或服务交换方式。它是 **XBridge**、**XChat** 和至少两个钱包或区块链节点的编排，采用的是 Noel Tiernan 原子交换协议的一般实现。该协议充分利用机密信息的创建，必须掌握此方面的知识方可花费资金，*并且*在花费资金时必须披露这些知识。因此，如果其创建者花费交易方的资金，则交易方拥有该机密信息并可能花费创建者的资金作为交换。

*注意：分散交换*服务*不同于分散交换*应用程序 ***Block DX***，*后者不仅使用此服务，还使用多个****区块链服务****。*

先前的工作

该协议的第一个版本被证明容易受到 m 基于延展性的勒索攻击，该问题后来在比特币与克隆生态系统中通过引入操作码 OP_CHECKLOCKTIMEVERIFY 得到纠正。Kay Kurokawa 关于此主题的博客详细介绍了利用后者的设计。最后，为了不仅支持加密货币和令牌的原子交换，还支持任何数字有效载荷，我们在该协议中添加使用解密密钥或安全的哈希功能*作为*机密信息。因此，揭示该机密信息即可立即使用先前提供的加密数字商品，或者验证某些真相。此方法与前一节中的零知识证明使用相结合，以允许消费者在接收数字商品之前验证其可信性，从而实现*对货币化商品和服务的可靠使用*。因此，这是一个*通用的*货币化服务协议。

协议步骤

从概念上讲，协议步骤如下：

1. 服务提供商创建解密密钥（用于数字商品）、数字签名或某些文件的加密哈希（用于真实验证）或随机数（用于数字货币交易），并将其用作协议的机密信息。
2. 服务提供商创建一个“保释”交易，规则为“如果消费者提供机密信息，或者消费者和服务提供商都签署了交易，则该交易可以由消费者花费”（如果提供数字商品而不是数字货币，则只需要一定数量的数字货币来支付网络费用）。
3. 服务提供商以第二次“退款”交易的形式创建回退机制，规则为“将保释交易的输出发送到服务提供商的地址，但不得早于从现在开始的 (x) 时间量”。
4. 服务提供商要求消费者签署退款交易，以便满足保释交易中的第二项要求，即如果消费者和服务提供商签名，则可以兑现。
5. 消费者签署退款交易并将其退还给服务提供商。
    a. *注意：这使得服务提供商可以在规定时间段回收其数字货币（如果有的话），前提是消费者放弃交换或者其他因素导致交易无法完成。*
6. 服务提供商广播交换交易。
    a. *注意：消费者现在可以“花费”这笔交易，前提是其已被提供机密信息。*
7. 如第 2 步中所述，消费者为自己区块链上的数字货币创建“保释”交易。
    a. *注意：此交易需要透露*相同的*机密信息才能使用 - 在此阶段只有服务提供商才拥有此信息。*
8. 消费者创建自己的“退款”交易，如第 3 步中所述。
9. 消费者请求服务提供商签署她的退款交易，如第 4 步所述。
10. 服务提供商签署退款交易并将其退回给消费者。
    a. *注意：这使得消费者能够在服务提供商未兑换数字货币的情况下收回此资金，否则机密信息不会透露给消费者，并且她将因此无法在交易中使用该服务或接收数字货币。*
11. 消费者广播她的保释交易
    a. *注意：服务提供商现在可能花费消费者的数字货币，因为它拥有机密信息。*

b. *注意：通过花费消费者的数字货币，服务提供商公开透露该机密信息，因此消费者现在可以使用该服务。*

c. *注意：如果服务提供商更愿意取消交易，它可能会等到步骤 3 中的时间 x 并广播其退款交易。*

12. 服务提供商花费消费者的交换交易，透露其机密信息。

    a. *注意：如果服务提供商未能进行保释交易，那么消费者可能会广播她的退款交易，并在规定的时间段内收回数字货币。*

    b. *注意：服务提供商必须在退款交易中指定的时间段内花费消费者的保释交易，否则消费者可以自行退款。*

13. 消费者使用这个机密信息来消费服务提供商的保释交易，或者解密一个文件，又或者验证一个事实。

    a. *注意：在数字货币交易的情况下，消费者必须在退款交易中规定的期限内花费服务提供商的交换交易，否则服务提供商可以自行退款。*

请注意，上述协议应包括额外的补充步骤，在这些步骤中，**服务节点**针对原子交换的状态进行更新，以便 SPV 节点和依赖于其对等实体中继交易和消息的“轻量”客户端实现可靠的更新。

消息传递步骤

正如 Blocknet 的组件中所实施的那样，分散交换通常包含以下步骤：

1. 在消费者按照**链间消息传递**一节中的步骤接受服务之后，服务提供商执行协议步骤 1-3，然后通过 XChat 执行步骤 4
2. 消费者通过 XChat 执行协议步骤 5
3. 服务提供商通过其本地区块链网络执行协议步骤 6
4. 消费者执行议步骤 7-8，然后通过 XChat 执行步骤 9
5. 服务提供商通过 XChat 执行协议步骤 10
6. 消费者和服务提供商在其各自的本地区块链网络上执行协议步骤 11-13

注意这些步骤仅涉及分散交换*服务*。与大多数应用程序一样，分布式交换应用程序 Block DX 需要几个额外的（即非核心）服务才能起到交换的作用，特别是订单广播、订单匹配、反垃圾邮件措施、反 DOS 措施和交易费收取。

上下文图

上述步骤暗含了本地机器上各组件之间的如下关系：

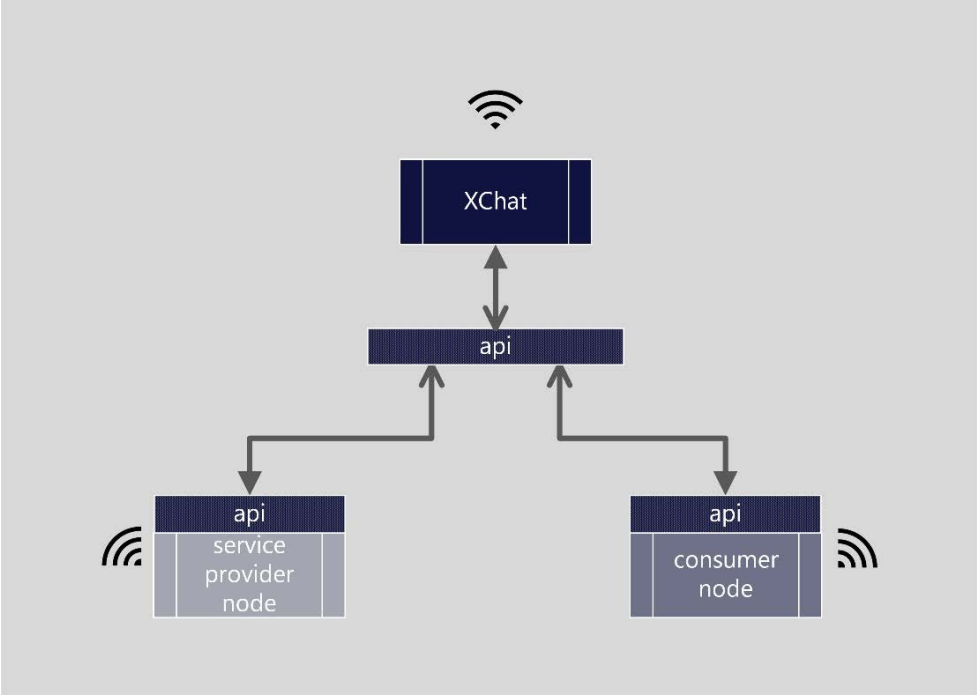


图 8
上下文图表明了本地机器上使用分散交换服务的核心组件的关系。

具体实施

目前：分散交换服务嵌入在 Blocknet 钱包中，并且位于独立的 Xbridgep2p.exe 中（然而，后期将对后者重新开发）。提供 API，同时支持分散交换*应用*。

未来：该服务应从 Block DX 使用的各种区块链服务中抽象出来，以及构建用于编排 XChat 和区块链服务的 API 外观。

区块链组件

在给定的本地机器上，上一节中介绍的三个核心服务可以与以下组件类型中的任何一个或组合进行交互，这些组件类型可能位于几个区块链上：

1. **全节点：**“常规的”全功能节点和钱包
2. **轻量节点：**SPV 节点和更轻量的节点（例如仅签署交易的节点）
3. **服务节点：**具有特殊功能的节点，用于提供超出常规区块链工作的给定服务

这些组件类型通常是不由 Blocknet 构建或维护的第三方集成。尽管如此，它们在 Blocknet 中提供了必要的功能，即与其本地区块链进行交互，否则 Blocknet 无法在不复制其自身组件的情况下实现互操作性 - 这将是一种无法实现的低效方法。

因此，三个核心组件和服务以及任何使用或交付链间服务的额外节点类型可表示如下：

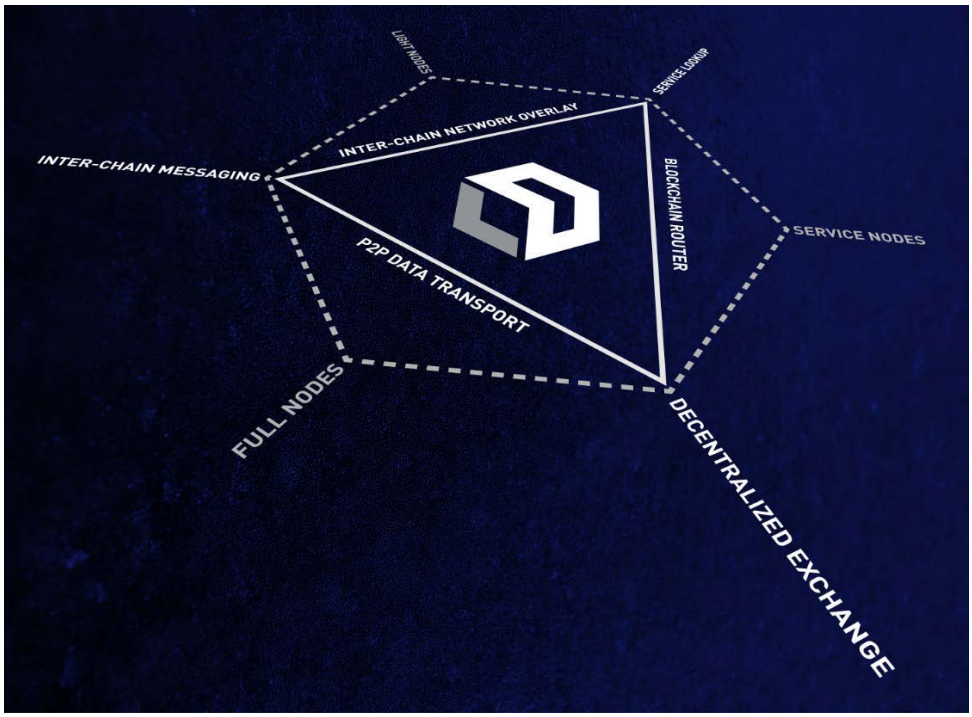


图 9
第三次迭代：
与三个核心服务和组件相关的区块链组件。
由于区块链组件使用核心服务，它们的关系表示为源自三角形的顶点。

区块链服务

区块链服务是对通用**核心服务**的补充，以支持特定使用案例。由于 Blocknet 上可能创建的链间服务数量没有限制，因此第三方可能构建的区块链服务数量也没有限制。

Block DX 是 Blocknet 上的第一个链间分布式应用，需要多个区块链服务。应当引入这些服务，以便记录它们，并说明区块链服务的性质。

BLOCK DX 区块链服务概述

作为交换的功能需要多种服务，以在交易方之间实现原子交换。事实上，任何交换（集中式或分散式）都必须提供四个关键功能：

- 资本存储
- 订单广播
- 订单匹配
- 结算

由于 Block DX 是一种分散交换，因此必然要求所有四个功能必须是分散式（除了涉及分散性的更广泛方面，例如维护完全开源的代码库，以及几乎每个人都可以列出数字货币）。借助原子交换，**分散的交换服务***以推理方式*分散了资本存储和结算。但是，原子交换并不等同于自身的交换；此外，订单广播和匹配必须分散。下面是区块链服务支持的功能：

- 订单广播通过利用**服务查找**服务进行分散，该服务完全是对等的。
- 订单匹配由每个交易者的分布式应用本地执行，它们是**核心组件**以及一个或多个区块链组件的编排。

订单广播和匹配的主要设计考虑因素是，像其他对等系统一样，它们自然容易遭受 DOS（拒绝服务）攻击。类似于比特币充当解决 Byzantine Generals 问题的电子现金系统功能，可行的解决方案必须达到订单簿上订单质量的保证。其次，令牌生态系统的设计考虑因素之一是如何使**使服务货币化**，因为在分散的生态系统中，如果商业模式不是经济上合理的，那么它们根本就不健全。接下来是这些问题的介绍性讨论，以及 Blocknet 针对它们提供的解决方案。

分散订单簿

注意：以下部分详细介绍了 Blocknet 的候选订单系统。虽然其他系统也在考虑之中，但包含当前的系统是为了引入分散式订单系统所在的设计空间，并鼓励在这一新领域发表评论和做出贡献。

订单簿类似于通告板，交易者可以通过在其上发布出价或询问来增加流动性，并且其他交易者可以通过使用投标或询问来获得流动性。除了在订单簿上发布订单的行为，一旦匹配成功，订单簿就会承担结算账目的责任。在分散的背景下，订单簿本质上变成了公告板，任何人都可以其中自由发布订单，没有中央控制人员发布信息，并且不会存在恶意交易。

因此，分散订单簿要求：(a) 确保只发布良好的订单（即必须防止订单垃圾邮件）；(b) 如果订单匹配，则交易方必须履行其定下的承诺（也就是说，它必须阻止订单 DOS）。现在，令人惊讶的是，区块链*并不是*一项用于订单簿的出色技术，原因有两点：首先，订单簿需要非常快速地运转 - 至少支持实时用户体验 - 但区块链需要交易（通常情况下是真实交易）在其真相得到充分确立之前至少位于链中的几个区块深处。其次，由于区块链需要挖掘来确立真相，这就使挖掘人员有机会获得订单信息的特权，并有可能取得竞争优势地位，因为如果他们挖掘下一个区块，则有利于其订单的匹配。因此，需要一个不同的系统来分散订单。

关于订单簿的最后一个新颖事实是，因为订单是对未来结算行为的承诺，所以在整个订单广播和匹配过程中不会发送任何资金或冒风险，从而使用订单系统的各方所承担的风险远小于支付或结算的风险。这在订单系统的设计中提供了优势，因为没有必要接受使用区块链会带来的严重性能损失；该系统可以成功运转，同时容忍一定程度的不真实。因此，作为*最低标准*，设计要求是防止非法活动扩展到孤立行为之外。具体来说，Blocknet 解决方案：

a) 支持 UTXO 验证，即订单中提供的数字货币是可消费的。
b) 使订单垃圾邮件不可展开，特别是采用对诚实交易者影响最小的杂凑现金式交易费，而这会使垃圾邮件花费巨大。
c) 采用与 (b) 中相同的方式，使订单 DOS 不可展开。
d) 使服务节点在经济上无法合谋（请参阅**服务节点的特殊属性**）。
e) 支持部分订单匹配，使多个交易方能够使用订单，而不会放弃一笔交易并锁定整个订单，直到退款交易变为可消费。这是交易策略的有效补充，通过在整个价格范围内将数据分散到多个订单上，避免交易方放弃单个高价值交易的机会成本。

分散订单的特征 - 自主权

我们认为，对于订单来说，分散性相当于维护分散交易行为主体之间的*自主权*。分散性不是一个很容易理解的术语，常常会与“分配”混为一谈，并且会与关于达成共识的概念混淆。Vitalik Buterin 明确解释，分散性基本上是关于*控制*：分散的制度不会将任何一方置于另一方的控制之下，除非所关注的问题是共享资源，在这种情况下，所有各方均平等参与。相比之下，分配只是在多方之间传播任务或角色，而不管是否有任何一方控制这一点。最后，各方之间的共识严格地涉及就事实或行动达成协议，而不是关于分配工作还是分散控制。然而，这并不意味着分散比特币不需要就哪些交易的合法性达成共识，而且这项工作并不是通过其网络边缘分配的。这些因素是必要的，但不足以让比特币分散。

分散货币与前面涉及*自主权*的分散订单类似：就像任何持有比特币的人都可以在没有第三方控制的情况下发送数字货币一样，任何交易者都可以向订单簿添加流动性或从中获取流动性；就像比特币用户可以证明给定数字货币是在特定时间发送一样，交易方可以自行验证订单和订单接受消息的有效性。然而，与加密货币的类比结束于考虑要*提供*订单以发送数字货币，这需要未来的交易方消费它们，并且涉及匹配过程。

因为匹配需要各方涉及相互签署订单接受消息，并且因为不需要*其他实体*来确定订单是否匹配，所以网络上的对等方可以在纯粹自主的基础上确定和发现订单状态，而不需要一致的算法（例如工作证明）。

我们提出一个涉及三方的完全自主的订单系统设计。下面是粗略的概述，随着讨论的进行，这些概述也将逐步发展：

- 在广播订单之前，造市者私下将订单和反垃圾邮件费用交易发送给服务节点，服务节点可以广播后者，花费数字货币作为网络费用，如果这是恶意行为，则花费造市者的费用。在验证费用交易后，服务节点将签署订单，这将成为市场接受者用于验证订单的证据。
- 当广播订单时，交易者可以自行验证 (a) 订单是由真实货币支持的，并且 (b) 已经由服务节点签署（表示已支付交易费）。
- 当一个或多个交易者试图接受订单时，制造者裁决这些请求（标准情况下接受第一个有效请求），并自行选择其交易方。
- 当选择交易对手时，造市者关注的是交易方不会 DOS 交易，因此它会等待服务节点验证交易费已经支付。
- 一旦服务节点广播一个已签名的接受消息，市场的其余部分就会通过删除订单来更新订单簿。

因此，Block DX 的订单簿充当分散的状态机。下图代表高层次的状态机（以下部分会介绍图中的某些细节）：

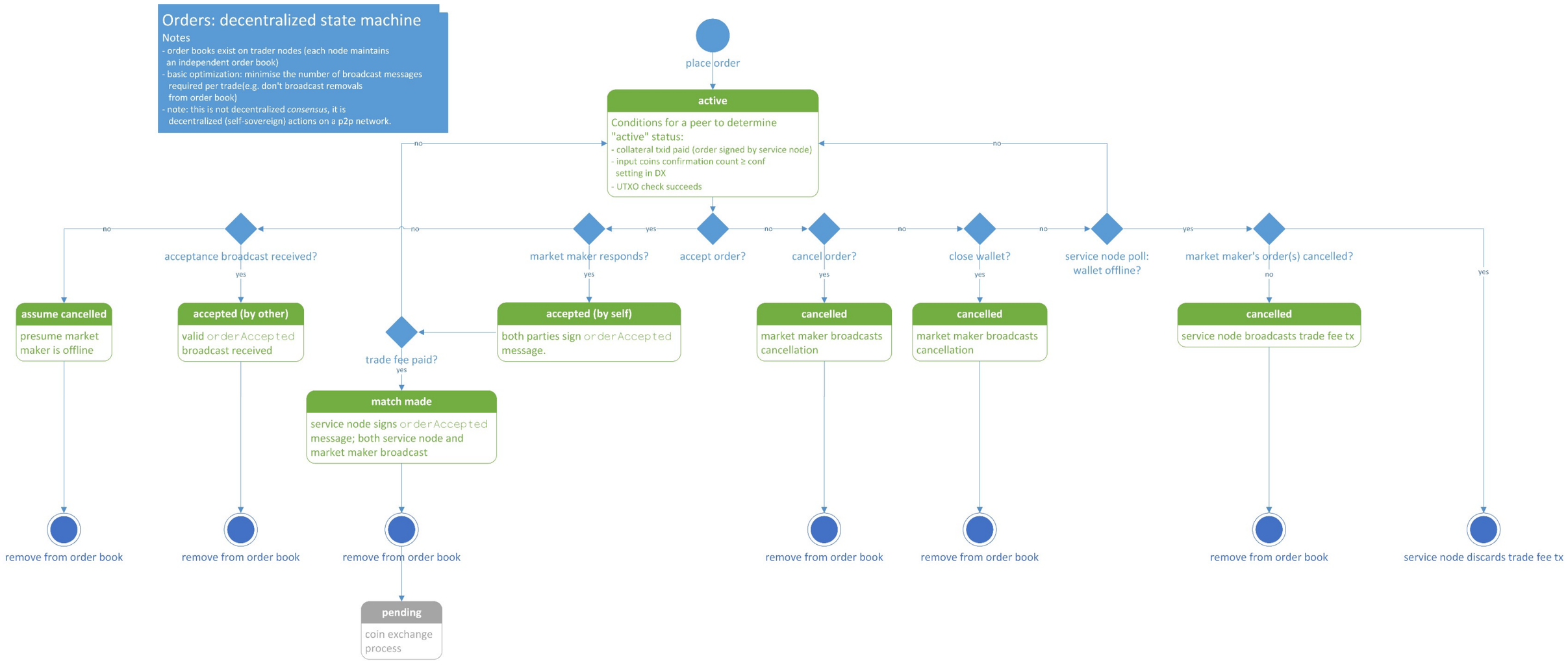


图 10
用于订单的分散状态机

角色分离：服务节点

Blocknet 的订单系统是一个三方系统，而不是简单地介于交易的两个交易方之间，这也许令人感到惊讶。但是，这是考虑到用户体验对收费影响的结果。例如，如果用户在下订单之前需要支付交易费，那么可以实施简单的分散式收费解决方案，但如果他们要取消订单，这也会导致他们被收取费用，即使交易方放弃交易。为了获得所需的行为（即，如果交易完成或取消，用户只需支付交易手续费），但同时需要在订购前支付费用，我们实行了三方制度。这是分离如下动机的结果：提供流动性，获取流动性，检查其交易方是否支付了费用，在没有 (a) 试图恶意地广播交易费交易时赚取交易费以及 (b) 除非订单被接受，否则不收取交易费。压倒一切的意图再次是自主权，这是通过分离和调整各方以特定方式行事的动机来得以维持的。这是一个复杂的系统，为了简单起见，每次只讨论一些考虑因素；在讨论的这个阶段，关键仅在于服务节点需要收取交易费，但在某一方于订单被接受之前取消订单时，不需要向它们收取费用（有关订单系统中的确切角色和顺序，请参阅下面的**详细协议草案**）。

服务节点的特殊特性

为了支持可靠的机制，在交易方于订单被接受之前取消订单时接受但不消费交易费（反垃圾邮件和反 DOS 的费用），服务节点具有几个新颖的特性。

1. 数量有限，易于识别

由于交易方将交易费用作为反垃圾邮件和反 DOS 措施，因此他们需要轻松确定是否支付了费用，这就要求能够区分由服务节点签署的订单（和订单接受消息）与其他节点签署的订单。

为此，我们要求服务节点保持 5000 个区块。这样，任何交易者都可以轻松扫描 5000 区块 UTXOS 的区块链并编译服务节点列表。然后，如果一个包含 5000 区块的地址验证了订单的签名，则表示它由服务节点签署。

2. 恶意行为会支付昂贵的费用

在开始赚取交易费用和区块奖励之前，服务节点应被要求保持至少 1000 个区块。如果服务节点采取恶意行为 - 即通过在用户合法取消订单时广播交易费用，则相关交易者可以向网络提交关于服务节点的黑名单证明声明。为了避开黑名单，需要将区块移动到一个新地址，在这种情况下，服务节点会因等待 1000 个区块的移动而损失很多交易费和区块奖励。

3. 恶意行为没有利润

除了恶意行为有很大机会带来昂贵成本之外，服务节点不能直接或可预测地从非法支付交易费中获益，因为交易费用被授予下一个获胜的中奖者，这有着一定的概率，并因此对于中奖者而言是不确定的。因此，服务节点没有实际的利益动机来实施恶意行为。

4. 支持可与 Blocknet 互操作的加密货币和令牌

为了验证订单或订单接受消息，需要服务节点验证订单中的地址是否包含足够的数字货币来为订单提供资金。因此，它们具有显著的硬件要求，因为其要求保持每个区块链的完整节点钱包可与 Blocknet 互操作。此要求进一步使服务节点能够在必要时为 SPV 和轻量节点中继消息和交易。

5. 没有机会实践内幕交易

因为任何服务节点都可能签署订单，所以服务节点所有者不可能为任何一个交易者（例如，她自己的交易节点）的订单授予特权，这是因为如果延迟签署其他人的订单（或订单接受消息），他们可能会从任何其他服务节点获得更出色的服务。

由于上述特性，交易者具有 (a) 信赖服务节点证词的“良好理由”，(b) 如果服务节点不能如实行事，则能够为服务节点造成收入损失，比交易费的损失要高昂多个数量级。(c) 如上所述，交易者在订单过程中遇到的较低风险，以及为获得更高可信度而施加的严厉表现惩罚，并不能够保证他们获得对订单的更高程度确信。

订单系统协议

假设前面对分散订单簿的一般性质和现实性的讨论是正确的，下面的协议草案就是其自然的解决方案。

1) 制造者准备交易费

a) 制造者想用 *y* BTC 购买 *x* LTC
b) 制造者计算 *tx* 费用（以区块方式支付）： $y * 0.05\% / price_{BLOCK}$
   i) 注意：$price_{BLOCK}$ 是发布订单时区块市场买入的平均买入价格。
   ii) 注意：区块应在下订单之前购买（为快速交易），例如在启动 DX 应用程序时 - 但仅在应用程序的区块供应量降至低于 1 个区块时。上面的步骤 (a) 简单地计算要花费的区块数量。
c) 制造者创建但不广播向造市者收取的交易费用 $tx_{spamfee}$，以防止订单垃圾邮件：
   i) 区块 tx
   ii) 其网络费用设置为正确的 (0.05%) 交易费用，
   iii) 并将输出作为制造者的地址。

2) 制造者张贴订单

a) 制造者创建一个订单，用 *y* BTC 购买 *x* LTC。填写如下字段：
   i) *y* 的值
   ii) *x* 的值
   iii) 为订单提供资金的 BTC 地址
   iv) 收取数字货币的 LTC 地址
   v) 制造者的 XChat 联系详情（地址、公钥）
   vi) [其他有用的数据：到期日等]
   vii) $tx_{spamfee}$ 的 txid
b) 制作商通过 XChat 将订单和 $tx_{spamfee}$ 发送到服务节点

c) 服务节点根据订单验证费用：
   i) $tx_{spamfee}$ 的 txid 与订单的 $tx_{spamfee}$ txid 字段相等
   ii) $tx_{spamfee}$ 网络费用是 *y* 的 0.05%
      (1) 注意：服务节点必须在 DX 上检查区块的价格以计算正确的费用；为了解释波动性，费用必须在正确值的 15% 以内。
   iii) $tx_{spamfee}$ BLOCK 地址可容纳足够的区块以涵盖费用。
   iv) 消费相同区块地址的内存池中没有 txs。
d) 服务节点签署订单。
e) 服务节点和制造者都广播订单+签名。
f) 服务节点在内存中保存 $tx_{spamfee}$，且不会立即广播。

3) 接受者准备交易费

a) 接受者想用 *x* LTC 购买 *y* BTC
   i) 注意：从用户体验的角度来看，接受者很可能会针对不同的数量设置市场或限价订单；此场景假定存在**匹配协议**以配对交易方之间的特定数量，从而部分填充订单。
b) 接受者计算 tx 费用（可按区块支付）：*x* * 0.2% / $price_{BLOCK}$
   i) 注意：$price_{BLOCK}$ 是接受订单时区块市场买入的平均买入价格。
   ii) 注意：区块应在下订单之前购买（便于快速交易），例如在启动 DX 应用程序时 - 但仅在应用程序的区块供应量降至低于 1 个区块时。上面的步骤 (a) 简单地计算要花费的区块数量。
c) 接受者创建但不广播 tx_{DOSfee}：
   i) 区块 tx
   ii) 其网络费用设置为正确的 (0.2%) 交易费用，
   iii) 并将输出作为接受者的地址。

4) 接受者接受订单

a) 接受者通过 XChat 向制造者发送订单接受消息。填写如下字段：
   i) 为订单提供资金的 LTC 地址
   ii) 收取数字货币的 BTC 地址
   iii) tx_{DOSfee} 的 txid
   iv) 使用 BTC 地址的私有密钥签署
b) 制造者验证接受消息：
   i) 使用对应制造者 BTC 地址的私有密钥进行有效签署
   ii) BTC 地址包含足够的余额
   iii) 从 BTC 地址消费的内存池中没有 txs
      (1) *信任注释：即使制造者可以验证接受消息，它也应在 tx_{DOSfee} 也由服务节点验证时方可继续，否则接受者可以免费 DOS 交换。*
c) 制造者签署订单接受消息
d) 服务节点验证订单接受消息：
      (1) 信任注释：制造者必须在服务节点之前验证接受信息，或者服务节点将 (a) 在找到对方之前以给定价格获得关于购买兴趣的信息，(b) 可以对任何一个接受消息进行特权验证，或者 (c) 可以使用任意标准阻止/过滤接受消息。
   ii) tx_{DOSfee} 的 txid 与接受消息的 tx_{DOSfee} txid 字段相等

iii) tx_{DOSfee} 网络费用是 *x* 的 0.2%

(1) 注意：服务节点必须在 DX 上检查区块的价格以计算正确的费用；为了解释波动性，费用必须在正确值的 15％ 以内。

iv) tx_{DOSfee} BLOCK 地址容纳足够的区块以涵盖费用。

v) 消费相同区块地址的内存池中没有 txs。

e) 服务节点签署接受消息

f) 服务节点和接受者都广播接受消息。

g) 每个交易者的订单簿都会将由制造者和服务节点签署的消息解析为订单状态从“打开”更改为“已填写”，并从订单簿中删除订单。

5) 继续进行保释 tx 设置

a) 根据原子交换协议。

广播交易费用交易的条件

在下列情况下，服务节点不得广播交易费用交易：

- 订单过期。
- 付款人在没有任何人接受订单的情况下关闭应用程序。
- 订单在接受之前被取消（上面的步骤 4f）。
- 交易方未能广播其保释交易。

订单匹配系统

Blocknet 需要一个分散的系统，用于 (a) 将交易的标准订单类型（市场、限价等）转换为基本的流动性消费活动，以及 (b) 以指定价格将一种数字货币的数量与另一种数字货币的数量相匹配。采用上面介绍的分散订单状态机 - 也就是说，如果相关方以制造者或接受者的身份获得自主权 - 订单匹配包括要求从制造者那里消费流动资金的接受者，并且在限价订单的情况下，订单缺乏直至达到某个阈值，以确定交易者作为制造者或接受者的角色。

市场订单的行为如下：在订单簿上消费订单，从最优价格的订单开始，转向次最优价格等，直到市场订单被完全消费。如果市场订单没有完全消费订单簿上的所有订单，则取消订单上的剩余金额。

限价订单的行为如下：如果订单是卖出，订单的价格低于订单簿上的最高（最低）还价（或者如果它是买入且订单的价格更高），则在该订单簿上消费订单，直到用户订单成为最低（最高）报价或完全消费。如果是前者，则将交易者的剩余订单添加到订单簿中。

为避免基于 UTXO 的加密货币发生更改的问题 - 以及需要在订单的其余部分进行交易之前等待变更确认 - XBridge 应自动将交易钱包的数字货币分配为不同地址的小额定期金额，以最大限度地提高交易方完全消费的产出数量，并将改动量降至最低。此外，应根据每个地址的金额大小规定最低交易额，以防止恶意创建改动。

交易历史服务

图表和其他技术分析工具需要数字货币之间的交易历史记录，并且一般来说交易者需要获得做出交易决策所需的市场信息。交易历史的真实性至关重要，因为如果仔细编制它，则可能会获得比其他交易者更大的优势。因此，任何给定货币对的交易历史应以“无需信任”的方式作为 Blocknet 服务提供。

下面的解决方案草案有点理想化，这是为了实现简化，并且为了展示主导思想而不是详细的技术解决方案；生产就绪解决方案将更加简洁（主要是由于未将交易历史数据本身包含在某个原子交换交易中），而是采用更复杂的零知识证明方案，例如防弹方案。

一个“无需信任”的数据集将需要 (a) 向其提交交易历史数据的适当真实方法，以及 (b) 从数据中检索数据的同等真实方法。该解决方案具体如下：

创建交易历史区块链，并且其节点在建立共识方面的工作相当于将来自其他区块链的贸易交易数据提交到交易历史区块链。提交的典型数据包括：

- 数字货币 A
- 数字货币 B
- 数字货币 A 的数量
- 数字货币 B 的数量
- 数字货币 A 的价格：数字货币 B
- 初次保释 tx 花费的时间

提交的数据必须足以让数据消费者以多种形式综合。例如对于 TradingView 图表，需要以下数据：

- 蜡烛期
- 蜡烛开始时间
- 开 始 价 格
- 结 束 价 格
- 高位价
- 低位价
- 等等

提交证明数据

要提交交易数据，交易历史区块链上的节点必须提交 *证明数据*：

- 数字货币 A
- 数字货币 B
- 在链 A 上花费的保释交易的 txid
- 在链 B 上花费的保释交易的 txid（如缺乏，则标记出来）
- 为造市者花费的交易费交易的 txid
- 为市场接受者花费的交易费交易的 txid
- 所以交易的时间戳
- 在其中提交证明数据的交易之时间戳

然后，由网络搜索交易中涉及的数字货币区块链并根据此区块链来验证节点提交的证明数据。节点也会参与重复数据删除，

其举措类似于数据挖掘，即网络必须确定第一个节点为特定交易提交证明数据，并丢弃其他节点提交的证明数据。

数据检索方法

有多种方式可以检索交易历史数据。交易者可以：

- 下载交易历史区块链，从而免费获取数据
- 在本地内存中存储所有完成的交易 - 这将需要连续运行 Block DX（实际上，这只会对实时更新图表有用）
- 请求交易历史链上节点的交易历史记录，具体为：
    - 特定数字货币对的费用
    - 一段时间内的费用

提供交易历史数据

为了向交易者提供交易历史，交易历史区块链上的节点必须提交：

- 在交易者指定的时间范围内针对数字货币 A、数字货币 B 和交易费用的所有 txid 的哈希
- 节点的地址

利用这些数据，交易者通过请求交易历史区块链上多个节点的交易历史记录，并验证所提供的哈希值是否相同，从而构建数据真实性的简单零知识证明（可参阅上面的注释）。如果结果是相同的，那么这相当于数据不真实的可能性很低，因为节点没有充分的理由互相信任，因此不具备恶意合谋的可能性。如果交易者希望更深入确定数据的真实性，他可以从模式节点请求交易历史记录，或者自行下载区块链。节点可以进一步监视对方对交易者的反应，并通过提交他们对区块链中的记录不忠的证据来惩罚不诚实的节点；在此基础上，网络就可轻松对节点的不诚实和黑名单达成共识。

如果交易者对来自交易历史节点的响应满意，它将选择第一个节点来提供哈希，并开始具有以下属性的原子交换：

- 仅可使用如下方式消费的保释交易
    - 与节点提供的地址对应的私有秘钥，以及
    - 与所提供哈希值对应的交易历史数据
- （换句话说，交易历史数据充当原子交换中的机密信息）

因此，如果交易历史节点花费保释交易，则它必须透露交易历史数据，如此交易者才可接收它。同时，交易者的历史数据不能在没有交易者支付的情况下显示。

目前的简化草案有一些值得注意的特性：

- 所请求数据集的大小可能受交易格式中机密信息的最大字段长度限制。然后，如果交易者希望获得更长时间范围内的交易数据，则需要交易者提交多个请求，从而推动交易历史节点获得收益。
- 每个数据集的费用可以根据交易量进行动态调整，因为每单位时间更大的数量会减少某个最大数据集的时间跨度。
- 交易历史数据的轻度混淆是针对拦截所请求交易历史数据（一点交易历史节点揭示此数据）的其他交易者提供的：因为它们既没有交易对，也没有将时间框架包含在数据集中，所以这些数据对其他交易者来说不会有什么用处，并且合成起来会很昂贵和复杂。

- 交易历史数据的强烈混淆版本将通过在 XChat 上加密发送实现，并且原子交换中的机密信息也可用作数据的解密密钥。然而，这需要一个更复杂的零知识证明，即该草案中的一个证明（见上文）。

注册表服务

上述的交易历史服务似乎是一般性的，以便为链间服务提供可行的注册表服务。直观地说，在交易不是数字货币而是数字商品的情况下，**区块链路由**中的提交和查找阶段保持不变。此外，还需要交易历史节点过滤其区块链的交易记录，以查看链 ID 出现的最新记录，并编译结果链表及其相关服务 ID 列表。该列表将使用上一节中的协议交付，而不是交易历史。

项目阶段

以下部分概述了项目的长期过程，旨在衡量总体范围，而不是提供对发展里程碑的一系列承诺。必要时可发布具有明确定义里程碑的短期路线图。

生产 MVP

- 单一客户/节点
    - 区块链路由
    - XChat 协议
    - 服务货币化机制
    - 交易费分配机制
- 分散交换的分布式应用
    - 前端 UI
    - 市场、限价和止损订单
    - 订单簿
    - 订单历史
    - 用户开启订单
    - TradingView 图表集成
        - 使用每个用户的账户 API 凭据
    - 设置向导：自动钱包 API 和图表 API 配置
    - 风险控制（可接受的确认数量）
        - 过滤订单簿
        - 允许您尽快下订单
        - 改动处理：
            - 接受订单；返回改动
            - 在 x 分钟内改动不可消费
            - 进入适当的风险范围
            - 订单的风险范围随数字货币时间自动更新

阶段 2

- 模块化 xbridgep2p
    - 区块链路由模块
    - XChat 模块
    - 数字货币交换模块
    - 分散交换客户
- 所有模块化组件的 API
- 在交换协议中支持数据有效载荷
- 交换协议和 XChat 传输协议之间的简单互操作性（通过您自己的分布式应用控制）

阶段 3

- 支持更多的订单类型：追踪止损、OCO
- 支持在关闭应用程序后留下订单（订单提交给区块链）

阶段 4

- 协议增强：交换衍生市场（p2p 保证金贷款）
- 协议增强：通用衍生品市场

技术规格

为了便于维护以及保持底层文档的单一真实来源，本节已移至 GitHub。

消息序列

即将发布。请参阅 https://github.com/BlocknetDX/blocknet-docs

API 参考

请参阅 https://github.com/BlocknetDX/BlockDX/blob/master/doc/dx/dxapi.md

使用案例

一个尚不存在的生态系统的基础设施给想象带来了一些困难。“其有何作用？”是最常见的以设计为重点的问题，而正确的答案类似于“任何可以从令牌生态系统中受益的对象” - 这是最重要的一点。为获得不太抽象的答案，下面是 Blocknet 的一个简短使用案例：

1. 分散交换

加密令牌的分散交换实际上是 Blocknet 的核心服务，因为它对于任何其他服务的货币化都是必不可少的。

在易于使用的分布式应用用户界面中，这也是 Blocknet 的第一款消费产品，因为它满足了加密社区对分散交易技术的真正需求。

黑客攻击、欺诈、失败以及集中式加密交换的盗窃盛行导致 16 个比特币中就有 1 个被盗。

2. 区块链路由

区块链路由也是 Blocknet 的核心服务，因为链间流量必须可路由到其预定目的地。也就是说，它也可作为有价值的服务来使用，任何节点为了交付或使用链间服务都可能需要这些服务。Blocknet 的初始路由器 XBridge 目前提供免费服务，而且这种情况在未来可能会持续下去。

3. 链间消息传递

无论是作为聊天应用还是作为数据传输，链间消息传递都是令牌生态系统不可缺少的服务。与分散交换和区块链路由一样，这是一个核心 Blocknet 服务，并且以 "XChat" 的名称命名。它采用端到端加密方式，以对等形式存在，可用于数字商品和信息的超安全传送。目前是免费服务，并且（当前）与 XBridge 中的区块链路由一起打包提供。

4. 利用多个链的移动应用

一个足迹较小的移动应用很可能只有一个 SPV 节点及其本地区块链接令牌。因此，

- 它会使用服务，而不是其他数字货币
- 它使用的各种**区块链服务**应该运行 Blocknet 组件
- 当此应用请求服务时，服务应产生一个“机密信息”，这也是数字商品的解密密钥
- 该服务应发送数据，使应用能够构建商品合法性的零知识证明
- 应当在**原子交换**中创建一个保释交易
- 该服务应该花费保释金交易，并且最好以后再交易另一种数字货币

- 该应用由此收到机密信息并可能会使用该服务

5. 近乎完美的数字货币混合器

如 ZCash、ZCoin 或 Monero 之类的私人货币可以集成到 XBridge 中，可为私人货币自动交易任何货币，并将其重新转换为原始货币。由于分散交换不需要任何第三方信任用户的数据，并且原子交换不涉及交易方风险，其结果是近乎完美的私人货币混合服务。

6. 分散化市场应用

市场应用通常需要以下服务：(a) 顾客声誉和信息，(b) 交付过程，(c) 图像存储，(d) 物品清单。由于**上述原因**，建议采用微服务架构，从而获得利用多个区块链的优势。因此，一条链可以存储加密的客户信息（请参阅此列表中的第 13 项），使用 XBridge 接受任何加密货币中的付款，将图像存储在服务器上，并使用第三个链和钱包代码来显示物品清单和 UI 元素。其结果是可扩展的、可组合的一组服务，更容易对其进行修补、升级或替换。

7. 用于 ETHEREUM 智能合同的燃料转化器

使用分散交换，任何 Ethereum 合同都可以获得采用其他数字货币形式的“燃气”。

8. 真正分散的稳定数字货币

稳定的数字货币可以通过利用分散交换的交易记录在链上这一事实来维持其关联性。因此，可用的真实数据集可用于确定是否铸币或烧币（或冻结并解冻它们）以维持关联性。

9. 自主权身份和个人信息管理器

个人信息服务可以在配备有可撤销许可系统的给定区块链上记录加密的个人元数据。用户因此获得他们的个人信息自主权。从这一点来说，可以将此区块链整合到任何需要登录的网站或应用程序中，或者用户可以自愿将其元数据出售给广告商以获得微额付款，或者它可以支持护照/身份识别系统。定位于利用此使用案例的新兴技术是 Bitnation 和微软的 Coco 框架。

10. 供应链 2.0 解决方案

Blocknet 基础架构非常适合充当“供应链 2.0”支柱。各方通常发现自己处于不同的区块链中，需要互操作，并且他们可能通过利用 Blocknet 服务来实现这种互操作。因此，多链应用程序能够从多个链中读取数据，无论它们是否擅长处理提货单、产品制造数据（如物料清单、财务数据）等数据。通过比较来自多个来源的元数据，Blocknet 可以帮助公司限制攻击媒介，如发票欺骗和伪造证书。

11. IoT 基础设施

一些常年的 IoT 安全问题可以通过利用区块链技术并借助 Blocknet 在数千个区块链之间进行互操作来得以解决。粒度货币化的多样化时机也体现出来：例如，使用 SPV 钱包同时可以完成多条链上的批量交易。数据流因此可以令牌化，并且可能会激励节点从事公司大数据中的模式查找。

12. 应用内的广告服务

移动应用可能会通过筛选作为 Blocknet 服务交付给应用的广告来获取其用户令牌。随后，可以使用令牌来为应用的链间服务消费提供动力，同时为用户提供“免费”服务，但为服务提供商提供货币化服务。

13. 分散的 p2p 存储解决方案

基于区块链的存储解决方案（如 Storj）可能通过链间服务交付显著扩大其用户群体并实现货币化。

14. 无权限 ICO 平台

任何人都可以通过分散交换提供令牌销售，无需获得权限。

15. 面向分布式预算管理的商业案例工具

加密项目通常作为一个大众包商业案例 (ICO) 推出，其中预算与市场协商。然而，实际账户余额随着众包在价值变化中进行的加密货币的价格而波动。使用 Blocknet，开发人员可以管理链中令牌和账户的分配。此外，通过使用智能合同，可以管理其他硬币的支出和投资，并且一般而言，项目的业务计划将由合同进行编码和自动执行，具有完全透明度。

16. 跨公司集成 ERP、CRM、PLM 系统

Blocknet 基于 API 的简单集成可实现与集团类型和私有区块链（如 ORACLE 和 SAP）直接或间接的互操作性。

17. 价值互联网的基础设施

Blocknet 的链式基础设施应随着时间的推移越来越多地发挥作用，创造出一种内在真实、透明和公平可用的“价值互联网”。随着公司的总分和分类账逐渐通过区块链与其他公司的分类账进行交互，所产生的区块链网络将成为价值流和给定系统价值的完整表示。这可以在整个系统中实现先进和深入的价值意识，从而对金融体系带来相应的强大和深远的影响。