Particle Network：探索链抽象的必要性

作者：Paul Timofeev 来源：Shoal Research 翻译：善欧巴，本站

去中心化应用程序指的是区块链原生产品和服务，自智能合约和以太坊诞生以来就已经存在。然而，用户对基于区块链的产品和服务的采用增长速度明显缓慢，尤其是相对于 Web2 应用和服务而言。考虑到 Netflix 的成功，他们通过从实体 DVD 租赁转向数字服务和流媒体世界，利用了卓越的便利性和选择性，超越了 Blockbuster。用智能手机轻触即可掌控世界的便利性导致了移动应用程序的采用，这改变了人们与互联网互动的方式，极大地造福了社交网络。ChatGPT 超越Instagram 和 Tiktok 成为增长最快的应用程序，它利用自然语言处理 (NLP) 简化了聊天机器人用户体验，为几乎任何人都提供了一种利用人工智能的简单而强大方法。

这些突破性产品和服务及其成功的共同点在于，它们提供了比任何现有企业或竞争对手更好的用户体验。为了使去中心化应用程序取得类似的成功，链上用户体验必须尽可能无缝和便捷，远离当今常见的种子短语和碎片化链条的世界。

## 改变链上用户体验

链上用户体验的最终目标是用户无需了解任何底层区块链基础设施；任何人都可以在任何区块链上做任何事情，而无需经过艰苦的入职和桥接流程。然而，为了更好地理解这种设计的重要性，我们有必要了解当今账户的状态：链上账户最终是用户和区块链之间的桥梁，它存储链上余额并定义与任何区块链原生程序的所有活动和交互。在其历史上，大多数区块链都使用了外部拥有账户（EOA）模型，该模型由两部分组成：一个公钥作为接收资产的身份和参考点（钱包地址），一个私钥作为访问的主密码（种子短语）。钱包在技术上充当账户抽象服务，因为它们简化了一个或多个链上账户的管理。

尽管 EOA 以其简单性和赋予任何人自我保管权而闻名，但迄今为止，它们也严重阻碍了链上用户体验。EOA 最常见的缺点是，任何获得种子短语访问权限的人都可以访问钱包（对于那些将种子短语存储在 iCloud 等基于云的服务上的人来说，这种威胁就出现了），并且任何失去对种子短语访问权限和/或忘记种子短语的人将无法再在链上访问他们的资金。

实现这种链上用户体验的关键是抽象原语的出现，抽象原语是许多产品和服务，它们围绕着尽可能多地抽象出链上用户体验中引起摩擦的痛点而构建。这些可能以工具包和框架的形式出现，供开发人员在自己的网络或应用程序中实现，或直接面向用户的产品和服务。随着该领域的发展升温，推出自己的抽象原语的团队数量开始增长，实现无缝的链上用户体验可能比大多数人想象的要快，正如Vitalik 所建议的那样。但究竟是什么促成了这一突破呢？

账户抽象是指将链上账户的管理与最终用户分开。这一概念最初早在 2017 年就已出现，但在 2021 年ERC-4337提出之前，它一直难以获得任何关注。围绕账户抽象的努力最初促成了智能合约钱包（通常称为智能账户）的开发。在这种模式下，链上账户由智能合约管理，因此可以更具可编程性并针对用户需求进行优化。这开启了新的可能性，例如能够使用熟悉的社交登录信息注册账户、在不同的链上使用相同的资产支付 gas 费、能够一键执行多个跨链交易等等。

实现账户抽象的关键是开发执行抽象服务，其中链上交易的执行外包给称为解算器（也称为填充器或执行器）的专业服务提供商，以代表签名者实现最佳性能和交付。在这里，用户签署称为意图的链下消息，其中包含执行链上操作的指令，即交易履行请求。通过将交易的执行与其签名分开，用户可以更轻松地表达期望的结果，而私有内存池或竞争性解算器网络等后端解决方案有助于为用户提供最佳结算和价值。

### 终局：链式抽象

实现终极链上用户体验的另一个关键组件是跨不同区块链环境进行通信和交互的能力。从历史上看，用户依靠桥梁来满足这一需求，但随着时间的推移，事实证明，桥梁是风险和不安全性的一大来源。链抽象在账户和执行抽象的发展基础上进行迭代，同时在网络层引入新的基础设施，从而消除了跨不同区块链环境进行通信和交互的复杂性。请参阅 Shoal 的链抽象深度探索，全面了解该概念的基础知识和更广泛的链抽象格局。

链抽象是围绕一个共同目标所做出的努力的结晶：提供无缝的用户体验，让用户可以执行链上操作，而无需知道他们在特定时间使用的是哪个区块链。本报告探讨了 Particle Network 如何通过其新的链抽象堆栈来实现终极链上用户体验的开发。

# Particle Network案例研究

协议背景

在联合创始人王鹏宇和潘涛的带领下，Particle 于 2022 年作为钱包抽象服务提供商首次亮相，推出了一个堆栈，供开发人员创建非托管、嵌入 dApp 的钱包，这些钱包可以通过 MPC-TSS 技术利用社交登录。随着 ERC-4337 帐户抽象的出现，协议转向将 AA 堆栈纳入其现有的 WA 堆栈，利用智能合约钱包来增强帐户结构。这为BTC Connect的推出做好了准备，它通过原生比特币签名将 AA 服务引入 BTC 生态系统。现在，Particle 正在推出他们的第 1 层区块链，作为其全面、多方面的链抽象堆栈的一部分。

Particle Network 由一支由 30 多名全职员工组成的全球分布式团队开发，并与Berachain、Avalanche、Arbitrum、zkSync等公司建立了合作伙伴关系。该协议在由 Spartan Group 和 Gumi Crypto 领投的几轮种子轮融资中正式筹集了 2500 万美元，最近还获得了币安实验室的投资。

# 协议概述

Particle Network是基于Cosmos SDK构建的模块化Layer 1，它将作为高性能EVM兼容执行环境中跨链交易的协调和结算层。

Particle L1 是 Particle 更广泛的链抽象堆栈的一个组件，它由通用账户（提供简单的界面来统一不同链之间的代币余额）、通用流动性（在后端启用 UA）和通用 Gas（允许用户使用他们持有的任何代币支付 gas 费用）组成。

Particle Network 的最终目标是在账户级别统一所有链上的用户，通过任何 L1、L2 或 L3 上的单一余额和账户实现无缝跨链交互，并允许任何人以他们想要的任何代币轻松支付 gas 费用。让我们仔细看看帮助实现这一目标的各种关键组件。

### 通用账户



通用账户是指由 Particle L1 提供支持的新账户结构，是 Particle 链抽象堆栈的关键。UA 的核心是附加到预先存在的 EOA（外部拥有地址）的 ERC-4337 智能账户，通过自动路由和执行原子跨链交易来统一多条链上的代币余额。对于最终用户，UA 提供了一个用于管理资金和跨各种 dApp 进行交易的单一界面，消除了在新的链上设置和资助新账户所涉及的摩擦痛点，这通常还需要购买该原生链的 gas 代币。

该接口建立在现有钱包之上，并利用 Particle 的流动性层——Universal Liquidity——执行原子跨链交易，并根据需要将用户余额中的资金路由到不同的链上。交易由 Particle 的全球分布式节点网络处理，这些节点管理相关的捆绑、中继和验证任务。

为了更好地说明，请考虑满足用户在外部链（链 X）上购买 Dogcoin 的简单请求所涉及的步骤：

用户通过现有的钱包或社交登录连接到他们的 UA。

用户向粒子 L1 提交他们的交易请求，表示为 ERC-4337 UserOp，以在链 X 上购买狗狗币。

Particle 分散式节点网络中的 Bundler 节点处理相关的 UserOp 并相应地执行它。

然后，Particle 的中继节点会监控并同步相关链上的执行状态。一旦确认交易已执行，状态就会从链路由回中继节点，中继节点会将状态传达给 UA 和最终用户。

我们的用户现在在他们的 UA 余额中拥有他们希望购买的代币，而无需与该代币所在的链进行交互。

显然，这里还有更多内部组件在工作，值得进一步检查。将 UA 视为 Particle 面向用户的产品。实现其提供的无缝体验的关键是 Universal Liquidity 和 Universal Gas 功能。

### 普遍流动性

通用流动性是指 Particle Network 中负责自动执行通过 UA 提交的交易的层。此功能由 Particle 的分布式 Bundler 节点网络提供支持，这些节点提供专门服务，启动执行 UserOp 所需的步骤，例如交换或从池中提取流动性。此外，分布式 Relayer 节点网络（称为去中心化消息网络 (DMN)）负责监控外部链（即目标链）上的交易状态并将其结算状态传回 Particle L1。

通用流动性的主要目的是使用户能够通过跨链交易与不同的链进行交互，而无需在相关链上购买和持有任何代币。为了更好地理解，请考虑以下流程，对于希望在链 D 上购买 100 USDC 的 Dogcoin 的用户，同时在链 A、B、C 和 D 上分别持有 25 USDC。

用户签署 UserOp 在链 D 上购买 100 USDC 的 Dogcoin，有效地将其在四条链（链 A、B、C、D）上的余额捆绑到由粒子 L1 处理的单个签名中。

执行签名后，用户在链 A、B 和 C 上持有的 USDC 将被发送给流动性提供者（否则理解为填充物）。

LP 在链 D 上释放全部 USDC 金额。

使用本地 DEX 将链 D 上的 USDC 兑换为 Dogcoin。

最终的狗狗币余额现已反映在用户的 UA 中。

### 通用Gas

通用 Gas 是 Particle 链抽象堆栈的第三大支柱，是实现gas 抽象的关键，其中获取和持有多个 gas 代币的摩擦痛点被从最终用户身上抽象出来，最终用户现在可以用任何链上的任何代币支付 gas 费用。Alice 可以使用她在 Base 上的 USDC 支付 Solana 上交换的 gas 费用，而 Bob 可以使用他在 Optimism 上的 OP 代币支付在以太坊上购买 NFT 的 gas 费用。

当用户希望通过 Particle UA 执行交易时，界面将提示用户选择他们想要的 gas 代币，然后该代币将自动通过 Particle 的原生 Paymaster 合约进行路由。所有 gas 付款都将结算到各自的源链和目标链，而部分费用将兑换成 Particle 的原生 $PARTI 代币，并在 Particle L1 上结算。



# 协议架构与设计



Particle L1 使用高性能 EVM 兼容执行环境和双代币质押模型来确保安全性，包括 BTC 和原生 PARTI 代币。共识和数据可用性外包给称为模块化节点的分布式节点网络。Particle 采用聚合数据可用性模型 (AggDA)，该模型可插入包括Celestia、Avail和 NearDA 在内的提供商组合，并由聚合 DA 节点运营商的去中心化系统提供支持。

在后端，Particle 的链抽象堆栈由三个关键模块提供支持：主密钥库中心、去中心化消息网络 (DMN) 和去中心化捆绑器。主密钥库中心充当Particle L1 中的中央事实来源，协调所有链上的智能合约部署，同步每个 UA 实例之间的设置，并维护所有链上的同步状态。DMN负责在用户进行交易的不同链之间传达交易执行状态，然后传达要在 Particle L1 上结算的用户操作的状态。此功能由中继节点网络提供支持。最后，Particle 利用去中心化的捆绑器网络，其中捆绑器节点运营商网络负责启动和执行传入的用户操作。该网络围绕分布式、无需许可的模块化节点网络构建，其中任务被委托和外包。

### 模块化节点

使用模块化节点将允许任何人参与运行专门用于促进 L1 上关键操作的节点。这些节点可以根据其各自的功能进行分类：捆绑器节点负责执行跨链用户操作，中继器节点负责监控并将交易状态（即已执行、失败）传达回要结算的粒子 L1，瞭望塔节点负责监控捆绑器和中继器网络中节点及其各自任务的状态，以及为每个时期的每个区块提供执行和欺诈证明。

### 聚合数据可用性模型

在区块链中，数据可用性 (DA) 是指验证已发布到区块链的数据的能力。通常，区块链将采用单一的 DA 解决方案，该解决方案可以在集成架构下内部完成，也可以在模块化架构下外包给合作伙伴或第三方提供商。Particle 正在构建其 DA 模型，通过采用聚合模型将 DA 外包给 Celestia、Avail 和 Near DA，以缓解其架构中的单点故障。Particle 采用两种不同的 DA 方法：选择性发布，将每个区块分配给单独的 DA 提供商；冗余发布，将每个单独的区块发送到每个 DA 提供商。



随着该领域的扩张，看看 Particle 未来是否会扩展到其他 DA 提供商（即 EigenDA）将会很有趣。

### 双重质押

使用权益证明模型的区块链会根据验证者在网络中质押的原生代币数量来分配验证者来提议和验证新区块，并根据他们投票的区块数量按比例奖励他们。这些网络在早期阶段面临的一个关键风险是原生代币的价格波动会影响网络安全性和稳定性。Particle 旨在通过双重质押模型来降低这种风险，该模型将通过Babylon质押协议利用 BTC 和原生 PARTI 代币，并为每个相应的代币分配验证者池。



### 使用通用 SDK 进行入门流程

Particle 的 Universal SDK 让应用程序开发人员能够创建无缝的 UA 入门流程，方法是让用户通过实施EIP-1193提供商来附加其现有钱包。这样一来，用户登录后便可立即从其 UA 进行交易。

利用 Particle Network 的Universal SDK 的应用程序内的入职流程如下所示。



# Particle Network状态

据该团队介绍，在开发 Particle L1之前，Particle 的钱包激活量已超过 1700 万次，用户操作量超过 1000 万次，并且与各种去中心化应用程序集成超过 900 次。

2024 年 5 月 2 日，Particle Network 的激励性 L1 测试网启动，通过Particle Pioneer平台提供积分奖励。Particle Network 的激励性公共测试网允许用户测试其旗舰级通用账户和通用 Gas 功能，以赚取积分来分配即将推出的 $PARTI 代币。

根据Particle Testnet V2 浏览器，130 万个区块中总共发生了 730 多万笔交易，平均每天超过 40 万笔交易。根据 Particle Pioneer活动网站，测试网已发生超过 1.82 亿笔交易，目前有超过 149 万用户共获得 273 亿积分，平均每位用户获得 18.3 万积分。Particle L1 目前计划于 2024 年下半年在主网上推出。

# 竞争格局

链抽象有望成为构建互操作性平台的下一个主要框架，并且即将出现的许多开发将与 Particle 竞争成为构建链抽象服务的标准工具包或堆栈。

### Near

Near 是一个分片式权益证明第 1 层区块链，为开发去中心化产品和服务的开发人员提供全栈应用领域。Near 正在构建其链抽象堆栈，即“帐户聚合”——一种多面结构，将用户的跨链交互汇集到单个帐户中。



Near 上的账户使用两种类型的密钥：完全访问密钥，其功能相当于私钥（即可以签署任何交易，但应保密）；函数调用密钥，其被授予对特定合约或合约集的专门签名调用的权限。Near 还利用其FastAuth登录服务，允许用户使用电子邮件注册账户，并使用生物识别技术代替密码。

实现此结构的关键是多链签名，它允许任何 Near 帐户与其他链上的地址进行交互。这是通过 NEAR MPC 网络实现的，该网络支持密钥重新共享，即使节点和密钥份额发生变化，公钥也保持不变。Near 网络中的 MPC 签名者节点允许智能合约启动签名过程，在任何链上创建大量远程地址。Near 还通过NEP-366引入了元交易，使用户无需持有原生 gas 代币即可跨多条链进行交易。这是由中继器（第三方提供商）实现的，它们将必要的 gas 费代币附加到他们中继到网络的签名交易中。

### Polygon

Polygon 正在开发AggLayer，这是使用 Polygon CDK 构建的 L2 统一桥，它将聚合 zk 证明并统一提交给以太坊进行结算。在此模型中，所有链都与其他受支持的 AggLayer 链共享桥合约，从而保持主权，同时受益于全球流动性中心，使引导早期网络变得更加容易。



AggLayer 将使用 ZK 证明来创建一个“感觉像一条链”的聚合环境，同时允许受支持的链保持其主权。应用程序开发人员可以从接触更多用户中受益，因为来自不同链的用户也将能够与他们的产品或服务进行交互。对于最终用户来说，目标与链抽象相同：提供类似于互联网的用户体验 - 一个不需要繁琐和频繁的桥接和其他复杂过程的单一环境。到目前为止，Polygon zkEVM 连接到的 AggLayer 的实时组件是 1) 一个统一的以太坊桥，用于实现跨链交易，以及 2) 一个 bridgeAndCall() solidity 合约库，用于帮助制定这些交易。

### Everclear

Everclear - Everclear 前身为 Connext，正在开发一种新的链抽象堆栈。顾名思义，Everclear 正在推出“第一个清算层”，以提供跨链交易的全球结算。Everclear 将作为由Gelato RaaS 提供支持的 Arbitrum Orbit L2 运行，并将使用 Hyperlane 和 Eigenlayer 连接到其他链。该协议最终充当协调跨链交易的共享计算机，结算以发票形式表示并通过荷兰式拍卖清算。这将围绕清算层的使用展开，“一个协调链间资本流动的全球净额结算和结算的去中心化网络”。Everclear 旨在为市场参与者降低成本，具有可编程性，可以插入任何交易的任何结算轨道，并从第一天起为新链和资产提供无需许可的流动性。

Socket -Socket 2.0标志着 Socket 协议从跨链服务向链抽象服务的转变，其旗舰模块化订单流拍卖 (MOFA) 机制是其一大亮点，旨在为高效的链抽象市场提供竞争机制。传统的 OFA 涉及一个由各种参与者组成的网络，这些参与者执行专门的任务，相互竞争，以提供针对最终用户请求的最佳结果。同样，MOFA 旨在为执行代理（称为发送器）和用户意图提供一个开放的市场。在 MOFA 中，发送器竞争创建和实现链抽象包或有序的用户请求序列，这些请求需要在多个区块链之间传输数据和价值。

### 未来展望

链抽象机会令人兴奋。然而，随着越来越多的团队开始推出自己的解决方案，风险投资公司开始将更多资金投入到任何提到“链抽象”的事物中，而用户开始绞尽脑汁思考哪种解决方案最好，有一些重要的考虑因素需要考虑。

## 抽象原语的案例

Zee Prime Capital 在最近的一篇文章中指出了有关抽象原语前景的几个重要考虑因素。

“如果没有产品，链抽象就不是解决实际问题的真正解决方案”。

诚然，虽然用户体验仍然是加密行业需要克服的关键障碍，但它可能不是吸引更多用户上链的最终瓶颈。事实上，基础设施的发展是为了应对高费用和缓慢结算造成的糟糕用户体验。现在基础设施已经存在（超过 200 个 L1/L2），但总体上缺乏在这些基础设施之上构建的成功产品和服务。这与Mert最近分享的观点一致，他声称没有足够多的人考虑到构建强大加密应用程序的障碍不是加密原生的（即基础设施、用户体验），而是围绕着整个行业的监管不明确和激励结构错位。

其中一个例子就是智能钱包的采用（或缺乏采用）。



尽管智能钱包带来了创新，但迄今为止，它们在很大程度上未能获得有意义的采用。在 2023 年第四季度/2024 年第一季度 memecoin 热潮开始时，Phantom 等现有应用创下了下载量记录，这表明人们愿意暂时处理种子短语和笨拙的用户界面，只要他们能得到最新的狗代币。

反过来说，使用新技术开发成功的产品和服务需要时间。第一批成功的基于 Web 的应用程序经过了多年的反复试验才出现。随着对基础层区块空间的需求不断增长，未来几年可能会出现更多汇总和特定于应用程序的链。随着 RaaS 提供商和 Celestia 等模块化基础设施解决方案的出现，启动新链和新环境将变得更加容易，这些环境将需要能够无缝地相互通信。将链从最终用户中抽象出来的需求来自于构建一个流行的应用程序，该应用程序将吸引其他链的用户想要使用它，从而促使需要服务来实现无缝体验。链抽象旨在解决缺乏无缝跨链功能的根本问题，而目前缺乏可用的产品和服务并不会使这一问题变得无效。

考虑到这一点，抽象原语必须应对的一个关键挑战是确保在状态证明、求解器执行、交易状态、区块确认和其他跨链保证方面在求解器/节点网络之间成功协调，所有这些都需要达成共识。资本市场的性质决定了另一种更快、更便宜的解决方案将永远出现，这意味着链抽象服务提供商必须考虑许多复杂的后端流程及其影响，其中诸如时间游戏和订单流捕获之类的东西随着时间的推移开始发挥更大的作用。

### Particle Network的重要考虑因素

Particle 分布式节点网络的一个关键问题是，这个网络的去中心化程度究竟有多高。只有少数实体参与运营节点，还是 Particle 能够获得足够的吸引力来维持一个足够去中心化的节点网络？Particle 如何才能成功激励足够多的节点运营商，使其首先变得足够去中心化？

为此，我们建议两点：

1）最大限度地降低节点运营商的进入和参与门槛

2）通过粒子浏览器提供公共仪表板，用于监控和观察节点网络的去中心化程度。

Particle 正在为原子跨链交易构建一个结算和协调层，其中通用账户取代了使用多个钱包、购买多个 gas 代币和桥接代币以在其他生态系统中使用 dApp 的需要。这带来了价值累积的问题；成功采用通用账户和 Particle L1 将对其他区块链和生态系统产生什么经济影响？他们会从更多用户访问他们的应用程序中受益吗？

## 链式抽象和Particle Network的案例

需要改变区块链原生应用程序的用户体验状态并不是一个新想法，开发人员已经研究这个问题有一段时间了。链抽象将通过创建更易于导航的链上体验使最终用户受益，通过为其应用程序解锁新用户群使应用程序开发人员受益，通过允许更便宜、更高效的跨链通信和路由使 L1/L2/L3 受益。

Particle 正在构建账户级链抽象以协助实现这一目标。通过将跨链交互统一到具有通用账户的单一界面中，允许用户使用通用流动性在任何链上进行交易，并使用通用 Gas 支付任何代币的 gas 费用，Particle Network L1 有望成为推动链抽象未来发展的领导者。

Vitalik 声称，他们“投入了大量精力和意愿”来实现无缝链上用户体验。单靠改善用户体验并不能带来数百万链上用户，但这是实现这一目标最重要的步骤之一。