一文详解 Particle Network如何通过多元化堆栈实现「通用」链抽象

作者：Paul Timofeev，Shoal Research；编译：Yangz，Techub News

去中心化应用指的是区块链原生产品和服务，自智能合约和以太坊问世以来就一直存在。然而，相对于 Web2 应用和服务而言，基于去中心化应用的用户采用速度还很缓慢。

Netflix 从实体 DVD 租赁到数字和流媒体服务的转变所带来的便利性和选择性，使其超越了 Blockbuster。而智能手机带来的「指尖上的世界 」的便利，促进了移动应用的采用，改变了人们与互联网交互的方式，极大地造福了社交网络。在当前人工智能的大环境下，ChatGPT超越Instagram 和 Tiktok 成为增长最快的应用，通过利用自然语言处理（NLP）的简化聊天机器人用户体验，为几乎所有人提供了简单而强大的人工智能利用方式。

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。去中心化应用要想取得类似的成功，链上用户体验也必须尽可能地无缝和便捷，远离当前常见的各种助记词和碎片化的区块链生态。

## 改变链上用户体验

链上用户体验的终极目标是，在用户无需了解任何底层区块链基础设施的情况下，允许任何人在任何区块链上做任何事情，且无复杂的门槛及后续繁琐的跨链流程。为了更好地理解这种设计的意义，我们有必要了解以下当前的链上账户状况。链上账户是用户与区块链之间的桥梁，在链上存储资产，并定义与任何区块链原生程序的所有活动和交互。截至目前，大多数区块链都采用外部拥有账户（EOA）模式，该模式由两部分组成，包括作为身份和接收资产参考点的公钥（钱包地址）和作为访问主密码的私钥（助记词）。而从技术上讲，钱包充当了账户抽象服务，简化了一个或多个链上账户的管理。

虽然 EOA 以其简单性和赋予任何人自我托管的权力而被广泛采用，但其也极大地阻碍了链上用户的体验。EOA 最常见的缺点是，任何人只要获得助记词的访问权限，就可以访问钱包（对于那些将助记词存储在 iCloud 等云服务上的人来说，这种威胁是存在的），而且任何人若是失去了助记词的访问权限或忘记了助记词，就无法再访问他们的链上资产。

提升这种链上用户体验的关键在于抽象原语的出现，即围绕尽可能抽象掉链上用户体验中的摩擦痛点而构建的许多产品和服务。它们可以是供开发者在自己的网络或应用中实施的工具包和框架，也可以是直接面向用户的产品和服务。正如Vitalik所言，随着这一领域的开发不断升温，推出自己的抽象原语的团队开始增多，实现无缝链上用户体验的时间可能比大多数人想象的要快。但究竟是什么促成了这一突破呢？

账户抽象指的是将链上账户的管理与终端用户分开。这一概念早在2017 年就已提出，但在 2021 年ERC-4337被提出之前，并没有获得关注。围绕账户抽象的努力最初促成了智能合约钱包的开发，也就是通常所说的智能账户。在这种模式下，链上账户由智能合约管理，因此可以根据用户需求进行更多编程和优化。这就带来了新的可能性，例如可以使用熟悉的社交登录注册账户，在不同的链上使用相同的资产支付 Gas 费，也可一键执行多个跨链交易等。

实现账户抽象化的关键是执行抽象服务的开发，即把链上交易的执行外包给称为解决者（solver，也称为 filler 或 executor）的专业服务提供商，以获得最佳方案并代表签名者执行交易。在这里，用户就链下信息进行签名被称为「意图」，其中包含执行链上操作（即交易执行请求）的指令。通过将交易执行与签名分离，用户可以更轻松地表达需求，而私有 mempool 或竞争性解决者网络等后端解决方案则有助于为用户提供最佳的结算和价值。

此外，实现终极链上用户体验的另一个关键要素是跨不同区块链环境进行通信和交互的能力。一直以来，用户依赖跨链桥来满足这一需求，但随着时间的推移，事实证明，跨链桥有着很大的风险，安全性不高。链抽象促进了围绕账户和执行抽象的开发，同时在网络层引入了新的基础设施，从而消除了在不同区块链环境中进行通信和交互的复杂性。有关该概念的基本原理和更广泛的链抽象生态的全面概述，可参阅 Shoal 的链抽象深度剖析。

链抽象是围绕一个共同目标所做努力的结晶，即提供无缝的用户体验，让用户可以执行链上操作，而无需知道自己在特定时间使用的是哪条链。下文将以 Particle Network 为例，探讨如何通过新的链抽象堆栈以促进链上用户体验。

## Particle Network 案例研究

### 协议背景

Particle，最初作为钱包抽象服务提供商，由联合创始人Pengyu Wang 和 Tao Pan 于 2022 年推出，为开发者推出了一个堆栈，可用于创建非托管、嵌入 DApp 的钱包，且可通过 MPC-TSS 技术利用社交账号进行登录。而随着 ERC-4337 账户抽象的出现，该协议将 AA 协议栈纳入了现有的 WA 协议栈，利用智能合约钱包增强了账户结构。这也为后来BTC Connect（通过本地比特币签名为比特币生态带来了 AA 服务）的推出奠定了基础。目前，作为其全面、多元链抽象堆栈的一部分，Particle 正在推出其 L1。

Particle Network 的开发团队遍布全球，有 30 多名全职员工，并与 Berachain、Avalanche、Arbitrum、zkSync 等公司建立了合作。该协议已在 Spartan Group 和 Gumi Crypto 领投的几轮种子轮融资中募集了 2500 万美元，最近还获得了 Binance Labs 的投资。

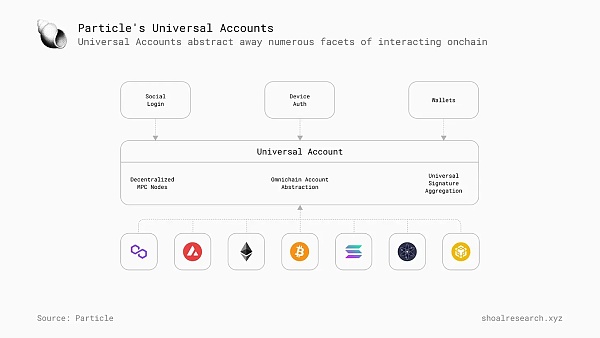
### 协议概述

Particle Network 是建立在 Cosmos SDK 基础上的模块化 L1，旨在于高性能 EVM 兼容执行环境中充当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成部分，该堆栈由通用账户（Universal Accounts）、通用流动性（Universal Liquidity）和通用 Gas（Universal Gas）组成。通用账户为统一不同链上的代币余额提供了一个简单的接口，通用流动性使用户可以在后端使用通用账户，而通用 Gas 使用户可以用他们持有的任何代币支付 Gas 费。

Particle Network 的最终目标是在账户层面上统一所有链上用户，通过 L1、L2 或 L3 上的单一余额和账户促进无缝的跨链交互，并允许任何人以其希望的任何代币轻松支付 Gas 费。

通用账户



通用账户（UA）是指由 Particle L1 支持的新账户结构，是 Particle 链抽象堆栈的关键。UA 的核心是附加到现有 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个链上的代币余额。对于终端用户来说，UA 提供了一个单一的界面，可用于管理资金并在不同的 dApp 之间进行交易，消除了在新的链上建立新账户并为其提供资金（通常还需要购买该原生链的 Gas 代币）所带来的摩擦。

该接口建立在现有钱包之上，利用 Particle 的通用流动性（Universal Liquidity）执行原子跨链交易，并根据需要将用户余额中的资金转移到不同的链上。交易由 Particle 的全球分布式节点网络处理，该网络管理相关的捆绑、中继和验证任务。

为了更好地说明这一点，我们可以设想一下要满足用户在外部链（X 链）上购买 Dogcoin 所涉及的步骤：

用户通过现有钱包或社交账号登录连接到他们的 UA。

用户向 Particle L1 提交交易请求，表达为在 X 链上购买 Dogcoin 的 ERC-4337 UserOp。

Particle 去中心化节点网络中的捆绑节点会处理相关的 UserOp 并相应执行。

然后，Particle 的中继器节点会监控并同步相关链上的执行状态。一旦交易被确认执行，状态就会从链上传回中继器节点，中继器节点再将状态传回用户协议和终端用户。

这样，在无需与代币所在的链进行交互的情况下，用户的 UA 余额中已经有了他们想要购买的代币。

当然，这一流程中还有更多内部组件的运作值得进一步研究。若将 UA 视为 Particle 面向用户的产品，那么通用流动性和通用 Gas 功能则是实现无缝体验的关键。

通用流动性

通用流动性（UL）指的是 Particle Network 中负责自动执行通过 UA 提交的交易的层。该层由 Particle 的分布式 Bundler 节点网络提供支持，这些节点提供专门服务，旨在执行用户操作（UserOp），如交易或从池中提取流动性。此外，一个由中继器节点组成的分布式网络，即去中心化消息传递网络（DMN）负责监控目标链上的交易状态，并将其结算状态传回 Particle L1。

UL 的主要目的是让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，可考虑以下流程：用户希望在链 D 上购买 100 USDC 的 Dogcoin，同时在链 A、B、C 和 D 上各持有 25 USDC。

首先，用户签署在链 D 上购买 100 USDC Dogcoin 的 UserOp，将其在四条链（链 A、B、C、D）上的余额捆绑到由 Particle 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（LP）。

LP 释放链 D 上的全部 USDC。

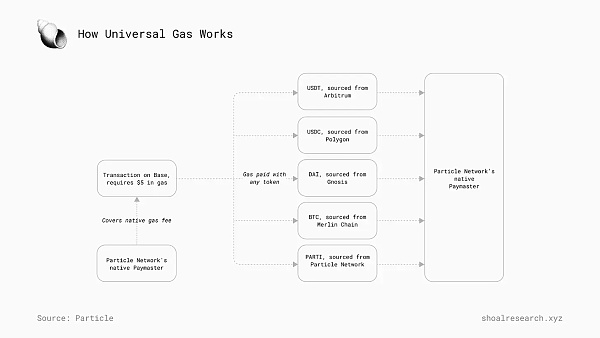
链 D 上的 USDC 通过本地 DEX 换成 Dogcoin。

最后，Dogcoin 余额就会出现在用户的 UA 中。

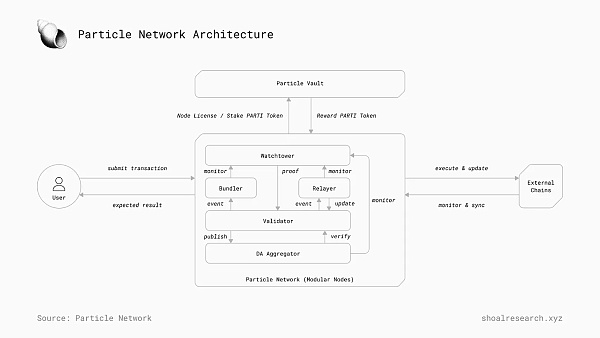
通用 Gas

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，允许终端用户在任何链上用任何代币支付 Gas 费用。比如，Alice 可以使用她在 Base 上的 USDC 支付 Solana 上的交易 Gas 费用，而 Bob 则可以使用他在 Optimism 上的 OP 代币支付购买以太坊上 NFT 的 Gas 费用。

当用户希望通过 Particle UA 执行交易时，会弹出一个界面提示用户选择 Gas 代币，然后自动通过 Particle 的原生 Paymaster 合约进行支付。所有 Gas 付款都会结算到各自的源链和目标链上，而部分费用则会换成 Particle 的原生 PARTI 代币，在 Particle L1 上结算。



### 协议架构和设计



Particle L1 采用了与 EVM 兼容的高性能执行环境和双代币质押模式，包括比特币和原生代币 PARTI 。共识和数据可用性外包给称为模块化节点（Modular Nodes）的分布式节点网络。Particle 采用聚合数据可用性模型（AggDA），该模型与 Celestia、Avail 和 Near DA 等提供商相结合，并由聚合 DA 节点操作员的去中心化系统提供支持。

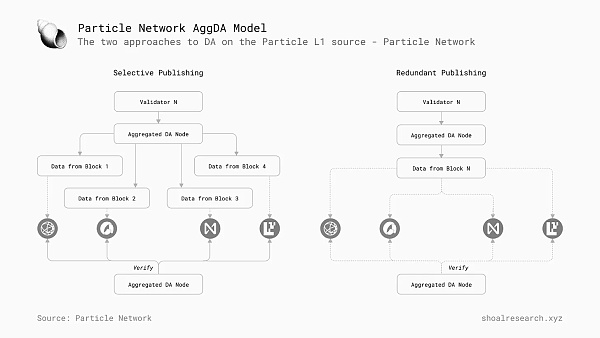
在后端，Particle 的链抽象堆栈由三个关键模块提供支持，包括主密钥存储枢纽（Master Keystore Hub）、去中心化消息传递网络（DMN）和去中心化捆绑（Decentralized Bundler）。主密钥库枢纽是整个 Particle L1 的核心信息源，负责协调所有链上的智能合约部署，同步每个 UA 实例之间的设置，并维护所有链上的同步状态。DMN 负责在用户正在进行交易的不同链上传达交易执行状态，然后将用户操作状态传达给 Particle L1，以便在 Particle L1 上进行结算。这一功能由中继器节点网络提供支持。最后，Particle 利用 Decentralized Bundler，由捆绑节点操作员网络负责启动和执行传入的用户操作。该网络围绕模块化节点（Modular Nodes）的分布式、无权限网络构建，任务在这些节点之间委派和外包。

### 模块化节点

模块化节点的使用允许任何人参与运行专门用于促进 L1 关键操作的节点。这些节点可根据各自的功能进行分类，比如捆绑节点负责执行跨链用户操作；中继节点负责监控交易状态（如已执行、失败）并将其传回 Particle L1 进行结算；监控节点（watchtower nodes）负责监控捆绑节点和中继节点网络中的节点及其各自任务的状态，并为每个区块每个 epoch 提供执行和欺诈证明。

### 聚合数据可用性模型

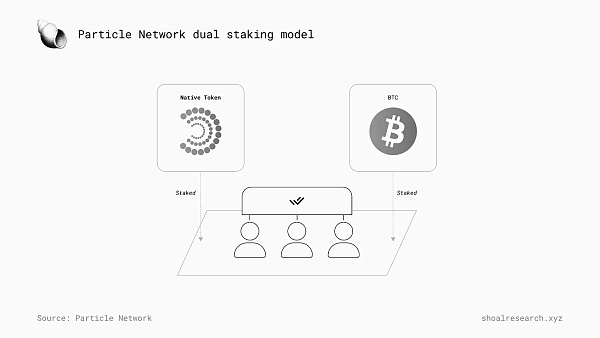
在区块链中，数据可用性（DA）是指验证已发布到区块链中的数据的能力。通常情况下，区块链会采用单一的数据可用性解决方案，这种解决方案可以是集成架构下的内部解决方案，也可以是模块化架构下外包给合作伙伴或第三方提供商的解决方案。Particle 正在构建其 DA 模型，通过采用聚合模型，将 DA 集体外包给 Celestia、Avail 和 Near DA，以减少整个架构中的单点故障。Particle 采用了两种不同的 DA 方法，包括选择性发布（将每个区块分配给单独的 DA 提供商）和冗余发布（将每个区块发送给每个 DA 提供商）。



随着该赛道的发展，Particle 未来是否会扩展到其他 DA 提供商（如 EigenDA），我们拭目以待。

### 双重质押

PoS 链会根据验证者质押的原生代币数量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给予奖励。在早期阶段，这些网络的一个主要风险是原生代币的价格波动会影响网络的安全性和稳定性。Particle 的目标是通过双重质押模式降低这种风险，允许质押原生 PARTI 代币，以及通过 Babylon 质押比特币。该模式会为每个代币分配验证池。



### 使用通用 SDK 的登录流程

Particle 的通用 SDK 允许用户通过支持 EIP-1193 的提供商来添加其现有钱包，从而使应用开发人员能够为 UA 创建一个无缝的登录流程，允许用户在登录后立即使用其 UA 进行交易。



## Particle Network 现状

据团队介绍，在开发 Particle L1 之前，Particle 的钱包激活次数超过 1700 万次， UserOp 超过 1000 万次，与 900 多个去中心化应用进行了。

2024 年 5 月 2 日，Particle Network 的激励 L1 测试网启动，通过 Particle Pioneer 平台提供积分奖励。该公共测试网允许用户测试其通用账户和通用 Gas 的功能，为即将发行的 PARTI 代币赚取积分。

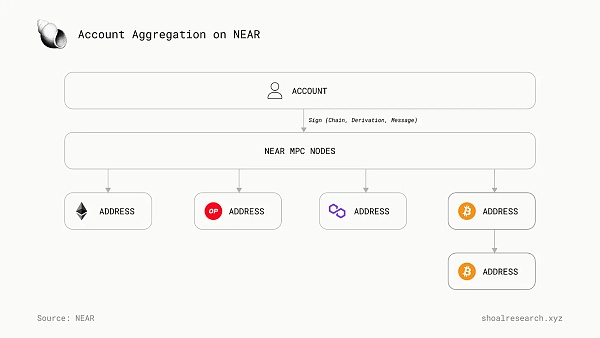
Particle Testnet V2 explorer数据显示，该网络已产生 130 万个区块，总交易量超过 730 万次，平均每日交易量超过 40 万次。此外，根据 Particle Pioneer活动网站，测试网的交易量已超 1.82 亿次，目前有超过 149 万用户，总计赚取了 273 亿积分，平均每个用户赚取 1.83 万个积分。Particle L1 目前计划于 2024 年下半年在主网推出。

### 链抽象赛道的竞争格局

链抽象有望成为互操作性平台构建的下一个主要框架。目前，该赛道已有多个项目旨在成为构建链抽象服务的标准工具包或堆栈。

### Near Network

Near 是一个分片式 PoS L1，正在通过账户聚合（Account Aggregation，一种多层面结构，可将用户的跨链交互通过单一账户运行）构建其链抽象堆栈。

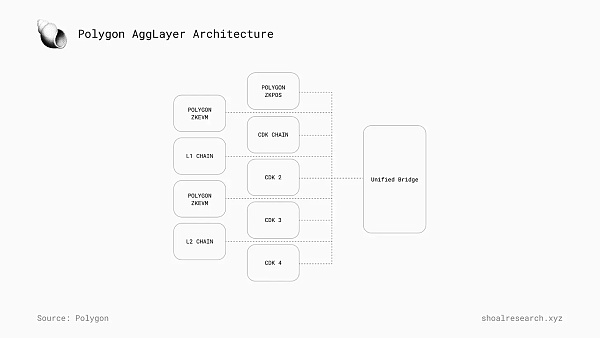


Near 上的账户使用两种密钥，其中完全访问密钥（Full-Access Keys）具有私钥功能（即可以签署任何交易），而功能调用密钥（Function-Call Keys）则被授予专门签署特定合约或合同集调用的权限。Near 还利用其 FastAuth 登录服务，允许用户使用电子邮件注册账户，并使用生物识别技术代替密码。

多链签名是实现这种结构的关键，它允许任何 Near 账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，即使节点和密钥分配发生变化，公钥也保持不变。Near network 中的 MPC 签名节点允许智能合约启动签名过程，从而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 代币即可在多个链上进行交易。这是由中继器（第三方提供商）实现的，它们将必要的 Gas 代币附加到了他们中继到网络的签名交易中。

### Polygon AggLayer

Polygon 正在开发 AggLayer，这是一个使用 Polygon CDK 为 L2 构建的统一跨链桥，可以聚合 zk 证明并统一提交给以太坊进行结算。在这种模式下，所有链都与其他受支持的 AggLayer 链共享一个跨链合约，可在保持独立性的情况下获得更多流动性，使早期网络的启动更加容易。



AggLayer 使用 ZK 证明来创建聚合环境，在让用户「感觉像在使用单一链」的同时，允许支持的链保持其独立性。此外，应用开发者可从接触到更多用户中获益，因为来自不同链的用户也可以与他们的产品或服务进行交互。对于终端用户来说，其目标与链抽象的目标相同，即提供类似互联网的用户体验。到目前为止，Polygon zkEVM 所连接的 AggLayer 的实时组件包括连接以太坊的统一跨链桥以及 solidity 合约的 bridgeAndCall() 库。

## 其他值得关注的项目

Everclear（前身是 Connext）正在开发一种新的链抽象堆栈。 顾名思义，Everclear 将推出「首个清算层」，为跨链交易提供全球结算。Everclear 将作为 Arbitrum Orbit L2 运行，由 Gelato RaaS 提供支持，并将使用 Hyperlane 和 Eigenlayer 与其他链连接。该协议最终旨在充当协调跨链交易的共享计算机，以发票形式结算，并通过荷兰式拍卖进行清算。Everclear 围绕其清算层（Clearing Layers）的使用展开，目标是降低市场参与者的成本。清算层是可编程的，可插入任何结算轨道，用于任何交易，且从第一天起就能为新的链和资产提供无许可的流动性。

Socket 2.0 标志着 Socket 协议已从跨链服务转向链抽象服务，其旗舰产品模块化订单流拍卖（MOFA）机制是这一转变的突出表现，该机制旨在为高效的链抽象市场提供竞争机制。传统的订单流拍卖涉及一个由执行专门任务的各种参与者组成的网络，他们通过竞争为终端用户的请求提供最佳结果。同样，MOFA 的目的是为被称为 Transmitter 的执行代理和用户意图提供一个开放的市场。在 MOFA 中，Transmitter 竞相创建并完成链抽象捆绑或用户请求的订单排序，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

链抽象赛道的机会令人兴奋。然而，随着越来越多的团队开始推出自己的解决方案，VC 开始将更多资金投入到任何提及「链抽象」的项目，且用户开始为选择哪种解决方案而苦恼，有一些重要因素值得我们考虑。

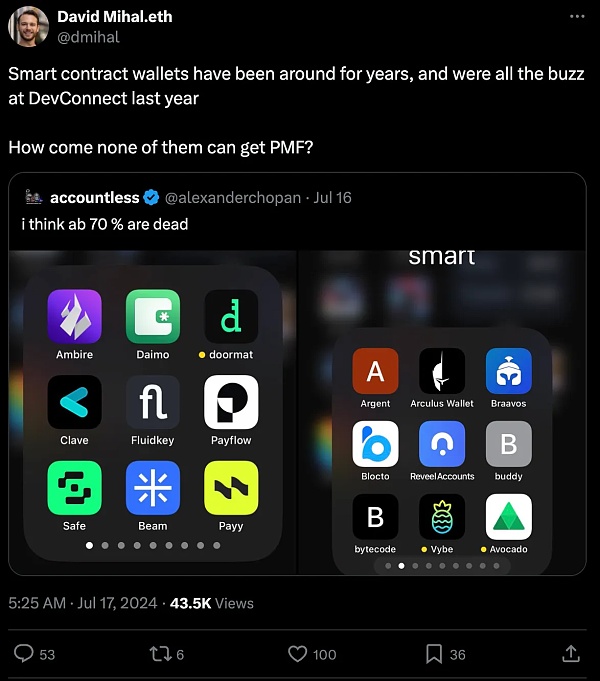
## 抽象原语的案例

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

「没有产品，链抽象就不能真正解决实际问题」。

的确，虽然用户体验仍然是加密货币行业需要克服的关键障碍，但它可能并不是将更多用户引入链上的最终瓶颈。事实上，基础设施的发展正是为了应对高昂的费用和缓慢的结算所带来的糟糕用户体验。现在，基础设施已经到位（已有超过 200 个 L1/L2），但在此基础上构建的成功产品和服务却不足。这与Mert最近分享的观点不谋而合，他认为目前大多数人还没有认识到，构建强大加密货币应用的障碍并不在于加密原生（即基础设施、用户体验），而在于整个行业的监管不明确和激励结构的错位。

一个很好的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，它们在很大程度上都未获得大规模采用。随着 2023 年第四季度/2024 年第一季度 memecoin 狂潮的袭来，Phantom 等现有应用的下载量创下了历史新高，这表明只要能买到新一代的「狗狗币」，人们暂时还愿意忍受纷繁的助记词和难用的 UI。

需要指出的是，利用新技术开发成功的产品和服务是需要时间的。基于网络的应用的成功就是经过多年的反复试验才实现的。随着对底层区块空间需求的增长，未来几年可能会出现更多的 Rollup 和应用链。而随着 RaaS 提供商和 Celestia 等模块化基础架构解决方案的出现，推出可无缝通信的新链只会变得更加容易。为终端用户提供链抽象的需求来自于创建一个可吸引他链用户且可提供无缝体验的热门应用。链抽象旨在解决缺乏无缝跨链功能这一根本问题，而目前缺乏可用产品和服务的情况并不会使其变得无效。

然而，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整个解决者/节点网络中成功协调状态证明、解决者执行、交易状态、区块确认和其他跨链保证，所有这些都需要达成共识。资本市场的性质决定了总会有下一种更快、更便宜的解决方案的出现，而这也意味着链抽象服务提供商必须考虑到一系列复杂的后端流程及其影响，随着时间的推移，诸如时间游戏和订单流捕获之类的东西将开始发挥更大的作用。

## Particle Network 需要考虑的重要因素

Particle 分布式节点网络的一个关键问题是，该网络的去中心化程度如何。是只有少数几个实体参与运营节点，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，使其实现充分的去中心化？

为此，我们提出两点建议：

1）尽量降低节点运营商的准入和参与门槛

2）通过 Particle 浏览器提供一个公共仪表板，用于监控和观察节点网络的去中心化情况

Particle 正在为原子跨链交易建立结算和协调层，而这也引出了价值积累的问题。通用账户和 Particle L1 的成功采用会对其他区块链和生态产生什么经济影响？它们是否能从更多用户访问中受益？

改变区块链原生应用的用户体验状态并不是一个新需求，为解决这个问题，开发人员已经研究了很长一段时间。链抽象可以为终端用户创造更易于使用的链上体验，可以为应用释放新的用户群，也可为 L1/L2/L3 提供更低成本和更高效的跨链通信和路由。

Vitalik 称，行业内的 builder 们有「大量精力和意愿」来实现无缝链上用户体验。仅靠改善用户体验并不能为行业带来数百万用户，但这仍是实现这一目标的最重要步骤之一。