钱包基础设施赋能下一代 Dapp

产品名称	钱包基础设施赋能下一代 Dapp
公司名称	河南漫云科技有限公司
价格	1000.00/件
规格参数	漫云科技:钱包基础设施赋能下一代 Dapp
公司地址	郑东新区升龙广场3号楼A座3202
联系电话	13103827627 13103827627

产品详情

到目前为止，用户在web3中进行次交互之前，必须安装额外的软件，使用一种新的货币为其提供资金并提供资金，并面临陌生的确认屏幕。尽管改进了防火墙并放弃了种子短语，但这些障碍仍然是去中心化应用程序的高流失率。

抽象技术层的创新环境已经成熟，可以直观地进入新的金融、社交和游戏体验，同时又不损害自我托管和去中心化的原始精神。

2023年是钱包生态系统的关键一年，账户抽象和堆栈各层的发展改变了市场结构，并改变了我们对用户、dapp和钱包之间关系的看法。

本文涵盖：

账户抽象及其好处

钱包基础设施和AA堆栈概述

新兴的dapp/钱包kaifa模式及其影响

持续的挑战和需要进一步探索的解决方案

账户抽象：什么、为什么以及如何

我们可以将账户抽象视为账户管理与密钥管理的解耦。账户是qukuailian上可以持有资产并具有交易历史的实体。签名者（密钥）是有权代表帐户执行操作的实体。

对于传统账户(EOA)，私钥保留对其关联账户的唯一且完全的控制权。私钥和账户之间严格的一一映射意味着：

用户在与qukuailian交互时只能使用专用的密钥管理解决方案（例如Metamask、Ledger）。

私钥丢失后无法追索，并且控制账户的密钥无法切换。

由该私钥发起的所有行为都被视为平等，从铸造免费的NFT到转移数百万美元。

账户抽象使账户成为一个智能合约，其动态逻辑决定哪些密钥可以代表其执行操作、范围权限以及根据用例进行额外的检查和平衡。

我们可以通过检查被抽象的内容来进一步分解它的好处。

由于以太坊协议仅识别EOA发起的交易，因此帐户抽象需要链下基础设施将智能合约发起的交易中继到链上。

ERC-4337于2021年推出，作为一种标准化方法，无需更改核心协议即可实现此目的。然而，早在标准完全充实之前，一些项目就已经发挥了AA的优势。

Safe*多重签名钱包于2017年推出，现已发展到为DAO、企业和个人等保护价值50B+美元的资产

Argent的手机钱包自2018年以来一直由智能合约账户提供支持

Sequence钱包于2021年推出，使Skyweaver能够使用电子邮件创建和登录智能账户，并使用非原生代币支付费用

这需要由相应的项目构建和维护自定义中继基础设施。

输入ERC-4337。该标准为中继层提供了一种去中心化且抗审查的替代方案，为帐户、付款人和签名聚合器定义了一个接口，以便通过帐户抽象交易的共享备用内存池（“ 用户操作 ”）与第三方中继器进行交互。

中继器（“ 捆绑器 ”）将多个UserOps捆绑在一起形成一个交易，发送到单个EntryPoint合约，该合约随后验证费用将被支付（由账户本身或通过付款人），并在对应于智能账户的UserOps上执行。

我们可以将其与验证和执行如何在原生提供账户抽象、因此不需要额外中继（例如zkSync*和Starknet）的链上进行对比，以及近发布的以太坊上原生AA及其汇总的RIP-7560提案。

2023年3月，4337EntryPoint合约部署到主网。它的社区在让kaifa人员参与帐户抽象运动方面取得了巨大成功。

这为钱包生态系统带来了一波新的基础设施和服务提供商浪潮，并推动了现有项目，以确保其业务战略和产品套件继续满足希望利用AA为用户提供无缝web3体验的应用程序kaifa人员的需求。

钱包基础设施和AA堆栈

签名者和密钥管理

签名者和密钥管理基础设施负责生成和保护用于签名消息、交易和UserOps的公钥对。这里直接的例子是传统的EOA钱包，但钱包即服务提供商已经出现，可以通过社交和电子邮件等替代身份验证方法实现无种子登录和钱包管理。

在幕后，这些服务要么将密钥材料存储在HSM中，例如AWSKMS，只有用户可以通过其身份验证凭证（Magic、Turnkey）访问这些密钥材料，要么在某些SSS/MPC方案（Privy、Web3Auth、Portal、Caps

ule）下运行以保护材料。

Lit*通过分散密钥来改进服务器端密钥存储设计。网络中的每个节点都存储一份通过DKG算法生成的ECDSA私钥，所有操作都在加密虚拟化中进行。可以将任意身份验证规则分配给密钥对，使应用程序或用户可以完全控制允许的交互，并施加支出限制等。2-of-NMPC钱包还可以进一步利用该网络作为备份和恢复选项。

今年，人们进行了快速实验，利用硬件签名者和密钥作为帐户的签名者，为用户提供现代移动或桌面设备开箱即用的密钥管理。这些签名者本机使用生物识别身份验证（例如FaceID、TouchID），通过熟悉的用户体验提供额外的安全性。

硬件签名者利用iPhoneSecureEnclave和AndroidTitanHSM等独立子系统来生成密钥和签名消息，从而保证硬件级安全。由于无法从设备中提取密钥，因此与其他恢复方法或作为2FA系统的一部分结合使用时，它的功能为强大。

密钥是构建在WebAuthn之上的无密码身份验证标准。在这里，密钥对是在设备的操作系统中生成的，并且可以通过iCloud等服务在设备之间同步，因此如果用户选择这样做，则可以进行恢复。

这里的一个限制是，密钥和硬件签名者生成的签名不能被bitebi和以太坊等链本机识别。他们使用secp256r1(R1)椭圆曲线，而这些链则在K1变体上运行。虽然正在进行以可信方式有效验证R1的工作，但一些支持Passkey的产品正在通过Lit和Turnkey等服务在用户使用其密钥进行身份验证后生成K1签名。

这里值得关注的标准是EIP-7212，它建议将R1曲线作为预编译合约直接添加到EVM中，以便每个现代设备都可以在没有第三方服务或中间人的情况下本地签署交易。

随着账户抽象交易量的增长，使用BLS签名的签名聚合可能会导致智能账户费用比L2上的EOA便宜。4337为聚合器辅助合约定义了一个接口，它验证批准多个UserOps的单个聚合签名，而不是单独验证每个用户操作。

中继器

中继器（例如4337Bundler）将事务或UserOps中继到内存池。在具有本机AA的链上，网络运营商和定序器扮演此角色，从而无需外部专用中继器。

与以太坊有多个客户端实现（例如geth、erigon、reth）类似，4337生态系统具有不同语言的多个捆绑器实现，使网络对单个实现的漏洞更加稳健。4337规范包括一个测试套件，以确保捆绑器在整个网络中的兼容性。实现者包括Stackup(Golang)、Pimlico、Biconomy、Etherspot(Typescript)、Candide(Python)、OKX(Java)和Alchemy(Rust)。

捆绑者的激励模型与区块构建者类似，从其捆绑的用户操作而不是交易中收取费用。在实践中，捆绑器需要一个进入块构建器的API来查看当前块并创建一个对该块有效的捆绑包，因此应将其视为块构建器的一部分。