深入探索Near协议的链抽象：基本组件和潜在新用例

作者：Cameron Dennis，NEAR协议核心贡献者；F.F，LBank Labs web3基础设施研究负责人；编译：本站xiaozou

## 1、引言

不同区块链、rollup和模块化组件的激增给Web3生态系统带来了极大的复杂性和严重的碎片化问题，让用户和开发者难以获得最佳体验，因为无数条各种各样的链会造成流动性、应用和用户的碎片化。相应而来的复杂的用户界面对于主流用户来说很难高效操作。

在不同链之间桥接资产通常少不了包装代币的混乱和非直观的过程。此外，跨链桥接机制不一致且繁琐，存在漏洞和安全风险。这种标准化的缺失不仅阻碍了资产的无缝转移，还使用户面临潜在的安全威胁。此外，各种链上的非原生资产的流动性通常是有限的，这进一步使资产转移过程复杂化。

最近的比特币复兴（Bitcoin Renaissance）主题活动产生了将智能合约功能引入链上的强烈需求，加剧了不同链之间的兼容性和互操作性方面的挑战。

为了实现大规模采用的愿景，一个统一的账户系统是必不可少的。该系统将允许用户与各种链上的应用程序无缝交互，自动桥接或交换资产。这消除了针对多个链单独管理各链账户的需要（每个链都需要不同的钱包接口）。使用单个NEAR帐户在任何链上签署交易的能力通过一个统一界面简化了用户交互，实现了无缝交易。

NEAR协议作为链抽象（Chain Abstraction）的全面解决方案脱颖而出，其核心重点是促进大规模采用。NEAR旨在降低用户的进入门槛，减少开发者的摩擦，并提供无缝的服务。它允许使用电子邮件地址创建和恢复帐户，无需获取资金即可使用帐户，并控制其他链上的帐户。尽管其底层系统很复杂，但NEAR提供了一个非常易用的平台，增强了用户体验。

本文的重点是深入研究NEAR链抽象的基本组件，包括帐户抽象（Account Abstraction）、前端抽象（Frontend Abstraction）和后端抽象（Backend Abstraction）。我们还将探索这些抽象层支持的潜在新用例。

## 2、登录抽象：原生域名系统

自2020年4月首次推出以来，NEAR协议的每个钱包都内置了账户抽象，它在过去一年中一直是以太坊生态系统中的一个突出话题，EIP 4337引发了大量讨论。然而，对于账户抽象这一概念的确切定义仍然缺乏共识。通常，人们倾向于在帐户抽象的保护伞下包含辅助功能，如社交登录、多签功能和gas费支付。从本质上讲，账户抽象指的是以编程方式建立交易的有效性条件并利用智能合约执行交易的能力。

而NEAR协议引入了一个原生域名系统，将人类可读的帐户与具有不同功能的不同权限的众多密钥相关联。NEAR还提供将外部账户（EOA）转换为智能合约的功能。因此，在其他区块链平台上被视为“账户抽象”的是NEAR架构的固有方面，是协议的内置功能。

### （1）.near是原始帐户抽象

. near账户模型构成了NEAR智能合约的基础，提供了高度可组合性和广泛的用户可能性。

FastAuth是一个关键的密钥管理系统，允许用户使用他们的电子邮件地址恢复或注册一个NEAR帐户。该功能提供了类似web2的登录体验，而无需存储助记词或密码。取而代之的是，密钥通过先进的“Passkeys”技术得到保护，该技术使用生物识别数据（如与特定设备相关联的指纹或FaceID）取代密码。用户可以通过MPC恢复服务随时使用他们的电子邮件重新访问他们的帐户。



FastAuth的下一个版本计划于本月发布，将包含NEAR地址到EVM、比特币和其他区块链地址的映射。该功能将使NEAR账户能够对其他链发起交易签名，从而直接在NEAR的智能合约环境中实现多链应用程序的无缝开发。

### （2）.tg开启新时代

每个NEAR帐户都可以与各种访问密钥对相关联。如果我们将NEAR帐户视为一个真实的人，那么这个人可以持有不同的密钥访问各种协议，甚至可以持有不同的密钥来使用不同的签名算法畅游不同的链。

由于NEAR基于WebAssembly的运行时，与Telegram的集成充分释放了它的潜力。到目前为止，NEAR协议的用户一直被限制在一个顶级域，.near。然而，.tg域的引入为大量的机会打开了大门。



领先的主流交易所已开始支持.tg账户的存取款，为更顺畅地整合其他顶级域名铺平了道路。

Telegram已被证明是通过HOT DAO（一个多链MPC网络，允许用户在Telegram上创建和管理钱包）实现大规模采用的网关。根据DappRadar的数据，HOT DAO在过去30天内平均每周有388万活跃用户。仅这款应用的周活跃用户就超过了Solana、Base和BNB的总和（2024年6月5日）。

这个钱包展示了用户体验可以类似熟悉的移动应用程序。此外，它还具有引入多链功能的能力，为用户提供链无关Dapp。

## 3、前端抽象

### （1）到NEAR协议的网关

Web Assembly驱动的区块链操作系统（BOS）标志着NEAR协议向开放网络（Open Web）迈出了开创性的一步。虽然NEAR不是第一个可以托管静态资源的公链，但却是第一个提出可组合的去中心化前端方法的公链。通过利用NEAR区块链具有成本效益的存储和计算能力，NEAR组件的代码完全链上存储在SocialDB智能合约内。

可组合的去中心化前端是指可与任何Web2或Web3后端以及任何钱包无缝集成的框架。BOS继承了React的设计，每个组件都构建在React组件之上。这种结构促进了精通JavaScript的大型开发者社区对开源代码库的贡献。值得注意的是，许多前端组件可以通过分叉协议再次使用，例如以Uniswap为模型的DEX平台。



除此之外，类似乐高积木的组件组合允许构建复杂的应用程序。这种方式简化了发布统一平台，为用户提供全面的体验，方便用户在单个页面上跨协议操作的过程。NEAR的官方网站near.org不仅是一个社交平台，还是开发人员的组件商店和用户的Dapp商店。

在讨论BOS时，NEAR组件和智能合约之间的互操作性经常被忽视。NEAR组件可以与NEAR区块链上的智能合约无缝交互。视图（view）方法允许任何人进行免费查询，而调用（call）方法则需要用户进行身份验证。

### （2）到L2的网关

去中心化前端可以提供易用的组件，以链抽象的方式进行构建。

DapDap作为以太坊L2的通用网关，提供了一个无缝且用户友好的平台，通过将其整合到单个UI中来简化整个DeFi的操作。DapDap支持10多个以太坊L2和超100个dApp，作为实现轻松登录和无缝探索开放网络的终极DeFi解决方案脱颖而出。



此外，DapDap不仅限于L2，EVM链的生态系统和协议本质上是相同的，包含去中心化交易所、借贷平台和NFT市场。这种统一性使创建一个跨各种EVM链的综合平台成为可能，为用户提供一站式解决方案，畅游去中心化金融空间。

## 4、后端抽象：链签名

### （1）TSS

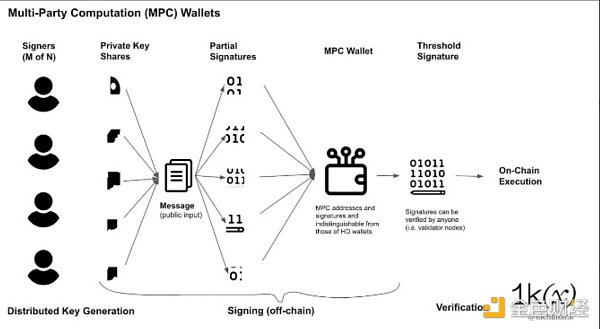
促进这一点的底层技术是链签名（Chain Signatures），这是一种开创性的阈值签名协议，它利用NEAR上的多方计算（MPC）签名者网络。

MPC并不是什么新鲜概念，已被用于Coinbase钱包等解决方案，其中用户保留一个密钥，中心化的各方保留其他密钥。MPC具有几个明显的优势：

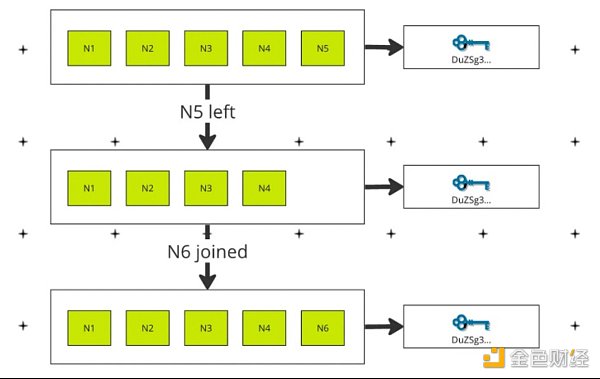
用户体验与传统应用程序保持一致。

MPC可以支持任何链，无论它是否支持智能合约（例如：比特币和Doge）。

它支持同时兼容多个链的底层椭圆曲线。例如，比特币和EVM使用基于ECDSA的曲线，而像NEAR、Solana和Cardano这样的链则使用EdDSA算法。

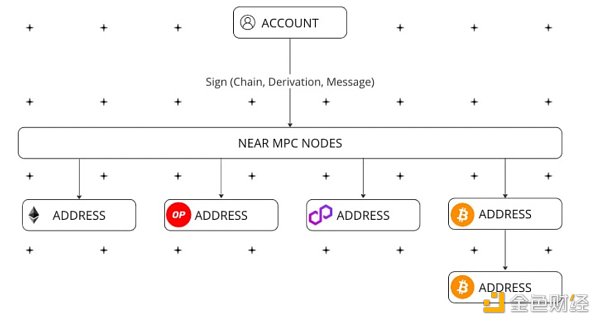


传统MPC签名方法的一个挑战是，更新节点需要生成新的公钥。然而，将新的阈值签名协议与密钥再共享过程集成，使MPC签名者能够维护相同的聚合公钥，即使密钥share和节点不断更新。



当将MPC应用于链签名时，每个链上的每个用户都会生成一个不同的地址，使他们能够将资产存入这些地址以进行无缝交换。

NEAR的一个关键优势是它的帐户模型，它本质上是一个控制一系列私钥的域名。智能合约钱包可以直接请求验证者签署任何任意有效载荷，例如比特币或Optimism上的交易。NEAR在其验证者间集成了可编程MPC功能。

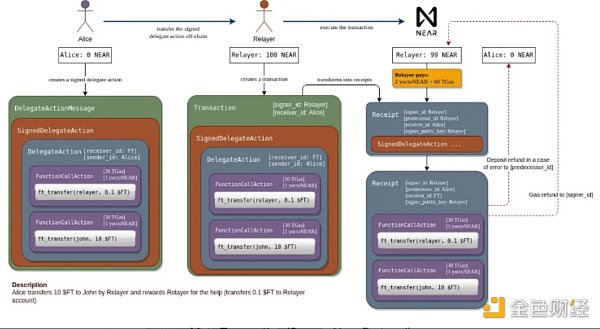


### （2）成熟的组件

元交易（Meta Transaction）

元交易是NEAR生态系统中的一种基本交易类型，支持用户在不拥有任何gas或代币的情况下在NEAR协议上进行交易。这个过程涉及到用户创建和授权链下交易，而由被称为relayer的第三方来支付提交和执行费用，从而简化了用户登录NEAR平台的过程。

元交易只与relayer一起时才能运作，relayer是一个链下操作的应用层概念。虽然realyer最初可能会免费提供服务，但若想长期可持续发展可能还需要其他付费模式。用户可以通过NEAR区块链以外的方法或在NEAR网络上使用可替代代币来补偿relayer。

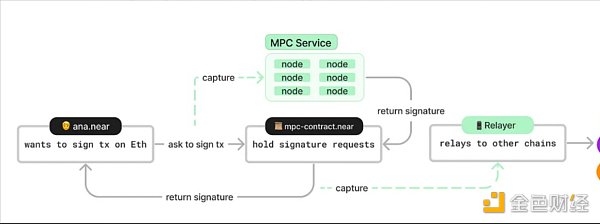


该特性为链抽象铺平了道路，引入的relayer在支持这一举措中起着至关重要的作用。Sweat是第一个采用此特性的协议，成功地将其数百万Web2用户转换为Web3用户。

意图Relayer

基于意图realyer开发建设，NEAR需要一个关键组件来支持跨异构链的用户交易：一个realyer网络。该网络监视来自多方计算（MPC）服务的响应，处理签名交易，并将其提交给各自对应链以完成交易。

该架构遵循基于意图的基础设施，其中NEAR包含复杂的多链意图网络。这种设置简化了生态系统项目中AI意图功能的集成，与即将到来的AI驱动的未来保持一致。

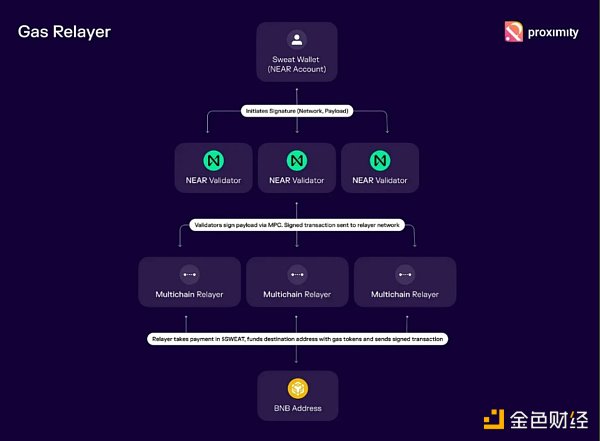


多链Gas Relayer

当与链签名一起使用时，多链gas relayer允许应用程序和用户避免跨不同链处理多个gas代币。它有效地管理各自链上的gas支付，使用户能够使用一种代币进行所有gas交易。

NEAR使钱包和应用程序开发人员能够探索各种选项，例如使用应用代币进行多链交易支付，实现固定费用订阅模式，或提供折扣以激励特定用户行为。

此外，Sweat Economy协议已经在测试网上展示了其功能，标志着一个重要的发展里程碑。

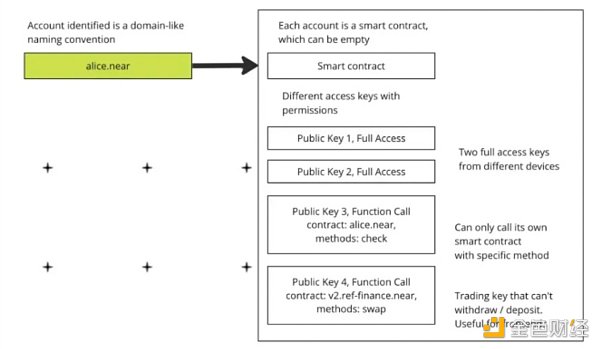


## 5、跨链dApp的新设计空间

目前，应用程序仅针对其单个发行链的用户群。然而，通过一个账户就可以在所有链上使用应用程序，为创始人和开发人员解锁了一系列之前极具挑战性的用例。

### （1）多链钱包

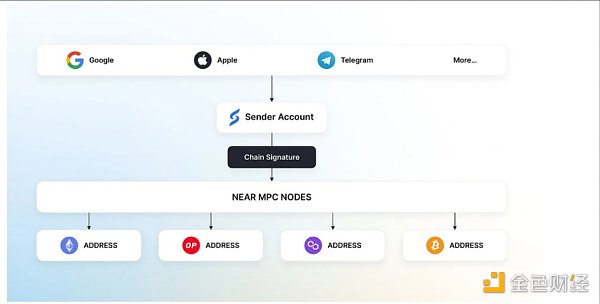
在NEAR帐户中，用户可以管理任意数量的密钥，支持密钥轮换以增强安全性，并实现多签名者模式。多链Gas Relayer进一步简化了与不同链的各种gas代币相关的复杂性。通过链签名，人们可以有效地“NEAR化”不同链上的账户，促进多链规模的账户抽象——从以太坊和Solana到比特币。



钱包开发人员可以轻松地利用NEAR的去中心化可组合接口，将所有链上的应用程序直接集成到他们的钱包体验中。例如，钱包就是这种集成的一个主要例子。

此外，帐户抽象功能提供了社交恢复的可能性。假设有一个维护与特定帐户root.near关联的好友记录的social—\_recovery.near合约。一开始，root.near帐户添加了一个公钥，social\_recovery.near账户可以通过链签名进行签名。好友可以通过将用户提供的新公钥转发给social\_recovery.near来启动恢复过程。在收到足够数量的此类请求后，social\_recovery.near就可以对一个NEAR交易进行签名，使用签名者root.near添加代表自己的远程密钥的新密钥。此交易一经执行，便立即向root.near添加一个新密钥，使用户能够通过他们为潜在的帐户恢复需求预先设置的社交恢复流程恢复他们的帐户。

Sender Wallet（发送人钱包）的概念承诺通过在若干基本方面简化私钥管理来彻底改变用户体验。首先，它提供从你的NEAR帐户即时生成的以太坊帐户来为用户简化流程。其次，它支持原子交换，允许NEAR账户和其他链之间的无缝交易，从而提高了交易效率。最后，Sender Wallet支持使用首选代币支付gas费，增强了交易管理的灵活性。



根据DappRadar，Here Wallet被公认为拥有最多唯一地址活动钱包（UAW）的领先dApp之一。

最初，Here Wallet推出了移动版钱包，旨在提供卓越的用户体验。然而，尽管存在优点，但它却难以获得实质性的牵引力。

最近通过Telegram向MPC钱包的转变完全改变了这种局面。Telegram拥有庞大的用户群，其中相当大一部分用户是加密领域的活跃参与者。这种转变意味着NEAR用户的自然增长，从而带来真正的用户粘性。

在加密货币领域，代币激励发挥着关键作用，比特币挖矿就是一个例子。事实证明，Here Wallet的HOT挖矿活动非常成功，在短短6个月内吸引了超过800万用户。HOT挖矿和推荐机制的吸引力最初成功吸引了用户，但由于Here Wallet不断推出新功能和应用程序——如HOT应用商店中的NFT市场MITTE——它们仍然会发挥作用继续探索生态系统。

### （2）非智能合约链生态系统

链签名使开发人员能够利用NEAR作为本身并不支持此功能的链的智能合约“层”。

NEAR智能合约可以作为托管合约，有效地管理所有权。基于这一基本功能，开发人员可以创建交换或借贷协议，以容纳各链资产，甚至是那些具有独特状态的资产。

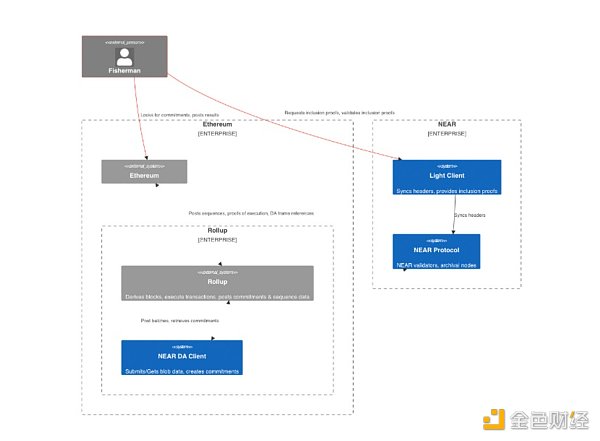
在East Blue的NEAR上运行的无需信任的比特币序数（Ordinals）市场系统中，工作流确保了卖家和买家之间安全透明的交易。卖家通过市场合约建立一个与他们的比特币钱包相关联的存款账户。市场合约专门要求MPC签名者代表比特币账户进行交易。在智能合约状态下，卖家对自己的比特币账户拥有所有权，允许它们存入和提取Ordinals。在存入并以10 USDC上架Ordinal后，如果一个活跃订单与它们的上架相关联，卖家将被限制提取该Ordinal。市场合约通过防止卖家进行未授权的提款来保护买家。反过来，买家将USDC存入市场合约，并继续接受指定的10 USDC上架。只有在双方确认同意账户互换交易后，才会执行交易，交易由市场合约在一个区块内自动处理。



## 6、数据抽象：NEAR DA

对NEAR的无缝区块链互操作性的愿景来说不可或缺的是其快速且低成本的数据可用性（DA）方法。随着Layer 2 rollup解决方案获得越来越多的关注，解决高效且经济的数据存储的挑战变得至关重要。NEAR的DA解决方案提供了一个全面的架构，经过精心设计，利用网络固有的高速和低成本，提供一个强大可扩展的为rollup数据量身定制的存储层。

NEAR DA的核心是Blob存储合约，这是一个专用智能合约，可以直接在NEAR区块链上去中心化存储任意DA blob。通过利用NEAR的共识和接收处理机制，该合约确保了高效安全的存储，而不会给共识层带来过多的数据负担。除这种创新的存储解决方案之外，还有Light Client，这是一个无需信任的链下组件，可支持KZG承诺、纠删码和存储连接器等高级功能。这个多功能的客户端可以让rollup供应商通过验证交易和收据包含证明来构建复杂的证明系统，进一步提高DA解决方案的可信度和透明度。此外，DA RPC Client作为与NEAR的DA系统无缝交互的主要接口，提供跨各种编程语言的一致且简洁的体验。



## 7、流动性抽象：无桥跨链DeFi

链签名最引人注目的一个方面是它们能够消除桥接需求，通过MPC签名协议促进跨链交易。用户对跨多链的DeFi平台有很高的需求。一些值得注意的用例有原生跨链交换（例如，将Ripple上的XRP兑换为Solana上的NFT），跨链借贷订单簿的实现（例如，利用Optimism上的X作为抵押品借入Arbitrum上的Y），以及在管理来自NEAR的相关奖励或罚没条件的同时，可以在任意链上再质押任意资产的能力。

这种能力对于像DapDap这样的应用程序来说尤其有价值，DapDap是基于NEAR协议开发的，允许用户在统一的界面内探索和参与不同L2解决方案的DeFi应用程序。虽然DapDap目前提供了与L2解决方案交互的链上前端组件，但用户仍然需要在MetaMask上切换网络设置来签署交易。如果用户可以简单地登录到他们的NEAR钱包，并在任何首选区块链上签署交易，会怎么样？

NEAR协议引入了一种新颖的解决方案，可能提供最具成本效益的链上资产交易方式，而无需担心比特币和以太坊等传统链上的高昂交易费和延迟问题。通过智能合约，用户可以交易衍生品路径，使他们能够交易存入远程账户的特定资产，而无需让整个账户参与交易过程。例如，去中心化交易所（DEX）可以在各链上保持资产所有权的路径衍生，并支持通过远程地址直接进行资产交易，而不会在其他区块链上产生结算费用。

## 8、结语：用户所有AI的先决条件

NEAR的链抽象为碎片化的区块链环境提供了一个解决方案，实现了所有链之间的无缝交互。这种方法结合了账户抽象、前端抽象、后端抽象、流动性抽象和数据抽象，使用户能够像使用他们最喜欢的集中式应用程序一样无缝地参与到去中心化生态系统中。

然而，NEAR的愿景远远超出了单纯的链互操作性。其最终目标是提供一个完全自主的操作系统，配备一个个人AI助手，在不损害隐私的情况下，根据用户的需求进行优化。该平台将支持个人用户所有AI之间的点对点交互和交易，同时还支持由各自成员管理的共享社区AI的建立。

这些社区AI将代表其成员的集体知识和需求，从小型俱乐部和初创企业到城市、全国、甚至是全球规模的社区。具有分叉现有社区和创建新社区的能力，并且由成员自己来管理，这个生态系统促进了创新和自决。通过选择性地管理用于训练的数据，并通过加密证明实现私有推理，这些社区模型确保了透明度和可验证性，为真正由人民拥有和控制的人工智能的未来铺平了道路。

随着NEAR生态系统的不断发展，其对利用可验证的、用户所有的人工智能潜力的关注将变得越来越重要。通过利用链抽象基础设施，NEAR有望促进超越区块链的创新AI应用程序的开发，使个人和社区能够塑造开放网络的未来。