Fiber Network：基于 CKB 的公共闪电网络

概述

Fiber Network 是一个基于 Nervos CKB 和链外通道构建的下一代公共闪电网络，可以为 RGB++ 资产提供快速、低成本和去中⼼化的多币种⽀付和点对点交易。

背景

区块链技术的发展与挑战

区块链技术自比特币问世以来，经历了迅猛的发展.从最初的简单支付功能，逐步扩展到智能合约、去中心化金融（DeFi）、非同质化代币（NFT）等广泛的应用领域。尽管区块链技术在安全性、透明度和去中心化方面具备显著优势，但其在扩展性和交易速度方面面临诸多挑战。

扩展性问题：传统区块链如比特币和以太坊在交易吞吐量上存在显著瓶颈。由于比特币的区块大小限制和 10 分钟的区块生成时间，其网络每秒只能处理约7笔交易；以太坊尽管有所改进，但每秒处理交易的能力也远低于传统支付网络。

高昂的交易费用：随着网络拥堵的加剧，交易费用显著上升。例如，以太坊网络上高峰期的 Gas 费用可能高于交易金额本身，这严重影响了用户体验并降低了小额支付的可行性。

交易确认时间长：在传统区块链网络中，交易需要等待多个区块确认才能被视为最终确认。这一过程可能耗时数分钟到数小时，不适用于即时支付的应用场景。

Nervos CKB 虽然在性能以及确认时间上有所改进，但仍然需要进一步提高交易速度和降低交易成本，以满足小额支付和即时支付的需求。

闪电网络的启示

闪电网络（Lightning Network）作为比特币网络的二层扩展解决方案，通过链下交易和支付通道技术，成功实现了快速、低成本的微支付。其核心理念包括：

支付通道：用户在链上创建支付通道，通道开启后，双方可以无限次地进行链下交易，只有在通道关闭时才进行链上结算。这显著减少了链上交易数量，提升了交易速度，降低了交易费用。

哈希时间锁合约（HTLC）：通过 HTLC 技术闪电网络可以确保资金的安全转移，避免交易对手风险。即使在链下交易失败的情况下，用户也能通过链上合约获得资金保障。

路由机制：闪电网络使用多跳路由，使得用户不需要与收款方开设直接通道即可完成支付，因此提高了网络的灵活性和可用性。

Nervos CKB 的优势

Nervos CKB 是一个专注于通用性和安全性的区块链平台。其独特的设计使其在解决区块链扩展性和互操作性问题上具备独特优势：

共识机制：基于 NC-Max[1]共识协议，同时在结合了工作量证明（PoW）和状态租赁机制，确保网络安全性和资源利用的有效性。

强大的智能合约模型：CKB 独有的 Cell 模型和 RISC-V 指令集虚拟机大大增强了 UTXO 模型的能力，不仅支持图灵完备的智能合约，还能轻松实现抽象账户以及 covenant 等特性，为去中心化应用提供了更灵活的可编程性，以及更好的互操作性和扩展性。

经济模型：CKB 的经济模型鼓励长期持有和合理使用网络资源，为去中心化应用，开发者和用户提供了安全可持续的去中心化生态环境。

Fiber Network 项目的意义

通过在 Nervos CKB 上构建链外通道，我们希望结合闪电网络的成功经验和 CKB 的技术优势，构建一个快速、低成本和去中心化的多资产实时支付交换网络。具体而言：

解决扩展性问题：通过链下支付通道和多跳路由技术，Fiber network 可以实现高吞吐量的交易处理，从而满足大规模用户的需求。

降低交易成本：减少链上交易频次，降低用户的交易费用，使得小额支付变得可行和高效。

提高交易速度：通过即时确认的链下交易，实现秒级支付确认体验，适用于各种即时支付场景。

多资产支持：支持多种数字资产的支付，为用户提供更广泛的支付选择。

支持网络互操作: 支持与比特币闪电网络的互操作，为跨链支付和资产转移提供支持。

架构设计

总体架构

Fiber Network 总体架构包括以下核心模块：

链下支付通道（Fiber Channels）

链上合约（HTLC）

多跳路由（Multi-Hop Routing）

监控服务（Watchtower Service）

链下支付通道

链下支付通道是 Fiber Network 的核心，通过它可以实现多次链下交易，仅在通道关闭时进行链上结算。这种机制显著减少了链上交易的数量，提高了交易速度和降低了交易费用。

大致的工作流程如下：

通道创建：双方用户在链上创建支付通道，锁定一定数量的 CKB 或者 RGB++ 资产。

链下交易：在通道开启期间，双方可以任意次进行链下交易，每次交易都更新通道状态，但不需要立即广播到链上。

通道关闭：当任一方决定关闭通道时，将最后的通道状态广播到链上进行结算，确保双方的最终余额得到确认。

具体的消息交互格式可以参考Fiber Network P2P Message Protocol[2]

链上合约

目前我们采用哈希时间锁合约（HTLC） 来确保链下交易的安全性并兼容闪电网络。通过它可以避免交易对手风险，确保即使在链下交易失败的情况下，用户也能通过链上合约获得资金保障。

大致的工作流程如下：

交易发起：支付发起方创建一个带有哈希锁定和时间锁定条件的交易，锁定一定数量的 CKB。

哈希验证：支付接收方必须在规定时间内提供正确的哈希原象，才能解锁交易，完成资金转移。

超时退款：如果接收方在规定时间内未能提供正确的哈希原象，交易将自动解锁并退款给支付发起方。

得益于 CKB 的图灵完备性，我们可以实现更灵活以及更安全的链上合约。之后会进一步扩展合约的功能，比如引入基于版本号的撤销机制和更安全的 Point Time-Locked Contracts。

多跳路由

多跳路由技术允许用户在没有和对方直接建立支付通道的情况下，通过多个中间节点完成支付。这种机制增强了网络的灵活性和覆盖范围。

工作流程：

路径发现：支付发起方通过路由模块发现从自身到支付接收方的最优路径。

路径锁定：在路径上的每个节点都创建相应的 HTLC 合约，确保资金安全转移。

支付完成：支付接收方解锁 HTLC，资金依次转移到路径上的各个节点。

同时我们也会在这里用HTLC合约实现跨链的支付，通过 cross-chain hub service 的方式来支持与闪电网络的互操作，具体可以参考Payment Channel Cross-Chain Protocol with HTLC[3]

监控服务

监控服务是 Fiber Network 的重要组成部分，它负责监控链下支付通道的状态，确保通道的安全性和资金的安全。功能和作用如下：

通道监控：实时监控所有参与用户的支付通道状态，包括通道创建、更新和关闭的过程。

异常检测：检测通道中的异常活动，如恶意用户试图以旧状态关闭通道或企图双花攻击。

主动响应：在检测到异常时，及时向区块链网络广播最新的通道状态，防止恶意行为导致的资金损失。

当前进展和计划

目前我们已经完成一个 Fiber Network 的原型，实现了两个节点之间的通道的创建、更新和关闭的基本功能，同时也验证了和比特币闪电网络做跨链的功能。项目代码可在这 2 个 GitHub 仓库中找到：

https://github.com/nervosnetwork/fiber

https://github.com/nervosnetwork/fiber-scripts

接下来的工作计划准备完成多跳路由和监控服务，以及完善 RPC 接口和 SDK，使得更多的开发者可以方便的接入 Fiber Network。

多跳路由协议基于 Dijkstra 算法来搜索支付路径，以此降低路由费用，并提高多跳路径支付成功率。在 Fiber Network 上线运行之后， 我们会根据网络流量和运行情况优化路由算法， 预计将会提供 2～3 种路径搜索策略，以适应用户不同的路由偏好和需求。Fiber Network 还将引入多路径支付策略，将较大的支付额分成多份，每一份由不同的路径传送，进一步增加支付成功概率。

监控服务将由 Fiber Network 中的一些节点提供， 他们保持在线，关注网络中的异常情况，帮助保护通道中的资产。监控服务还将追踪 cross-chain hub service。即使用户在一段时间内离线， 监控服务也能确保与闪电网络的交换能成功进行。

此外，我们还将考虑在 Fiber Network 中加入更多功能，比如，利用 CKB 的可编程性实现隐私保护算法， 并基于此优化路由算法和监控服务，保护用户支付信息的安全和隐私。