为什么要使用零知识证明来开发跨链协议？

在 Web3.0 多链生态里，用户在交互过程中并不想频繁切换钱包和网络，用户需要的是更安全、更通用、更友好的链间通信协议。

用户需要什么样的跨链服务？

在过去的几年当中出现了各种各样的独立公链以及以太坊 Layer 2。由于在安全性、低成本、快速交易以及开发者和用户社区差异等方面，不同链都具有各自不同的优势，用户在不同链之间切换使用的行为是很常见的。比起以太坊链，Layer2 以及其他独立公链上的手续费会更加便宜，并且交易速度也会更快。于是，用户为了降低交易成本或

者使用其他链上更优质或者独特的应用就必须使用跨链桥。

如果把跨链桥比喻成“运钞车”，那不管有没有人来抢运钞车，也不管采用什么手段来抢运钞车，运钞车本身都必须具有强大的防御能力，不能有任何安全问题。运钞车从设计、生产、制造环节不能出现问题，押送环节不能出现问题，发送、接收环节不能出问题。在现有跨链桥解决方案要么存在架构设计问题，要么存在代码漏洞问题，要么协议本身在收发和中继环节依赖于某种信任假设。以上这些都大大降低了跨链桥的安全性。

跨链桥作为搭建在各条公链上的桥梁，解决众多公链之间流动性割裂，毋庸置疑是资产跨链转移非常重要的解决方案。然而，用户对跨链技术的需求不会仅仅停留在资产跨链上，资产跨链其实只是整个跨链协议的 DeFi 赛道的一种应用。两个截然不同的网络通过跨链协议具有了互操作性，这种互操作性不仅需要实现代币在独立平台之间相互转移，而且需要实现大文件、数据包的链间通信。

在 Web3.0 多链生态里，用户其实只想通过一个应用就可以顺畅地与所有主流公链进行资产与数据的交互。在交互过程，用户并不想频繁切换钱包和网络。

在“一超多强”公链格局下，用户需要的是更安全、更通用、更友好

的链间通信协议。

有哪些跨链通信模式?

原生验证模式

本机验证是通过在源链和目标链的虚拟机中运行一个轻客户端，并通过中继器来进行链间通信。该模式的特点是不需要运营一条介于各条公链之间的链。如果像 Way Network 一样采用零知识证明，还可以摈除 LayerZero 所需要的信任假设。

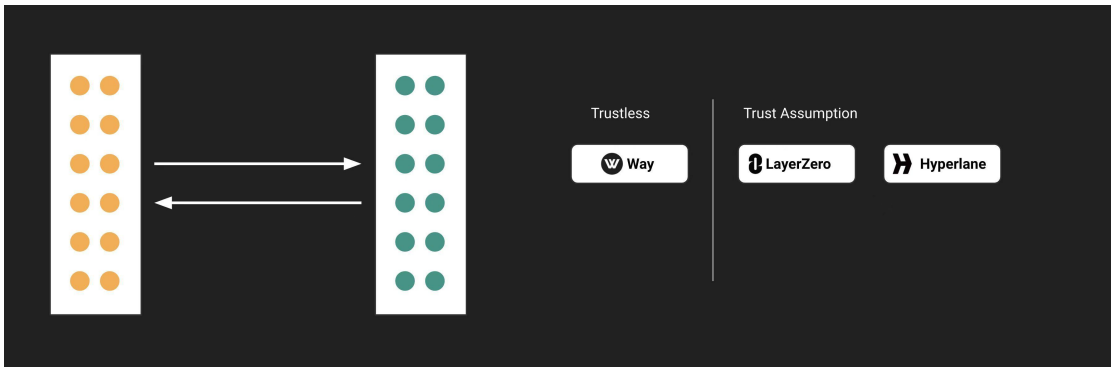

图 1：原生验证模式

外部验证模式

外部验证有一个或一组验证者，他们需要监视源链的特定地址。当用户将一个资产发送到源链上的特定地址时，该资产将被临时锁定。第

三方验证者验证该信息，并需要达成共识。当达成共识时，相应的资产将在目标链中生成。

这种通信模式的缺点是有“信任假设”，容易出现因为“单点故障”或者“局部故障”而导致资产被盗。

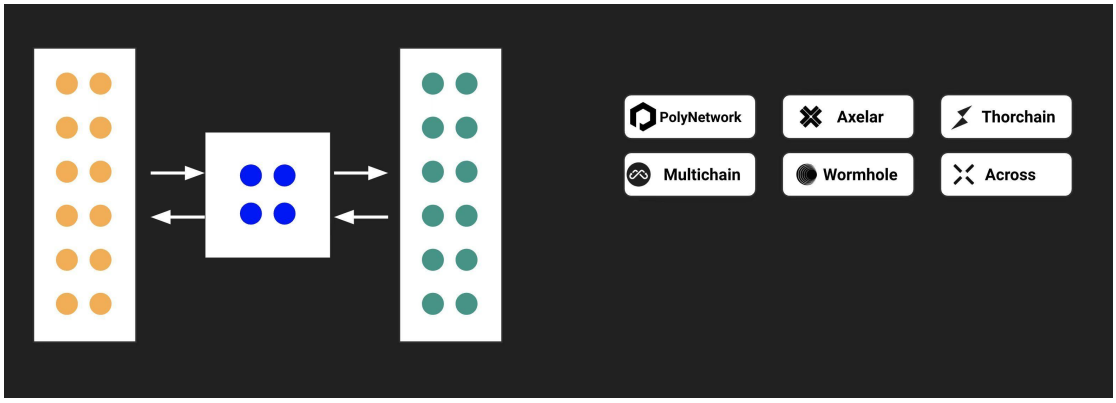

图 2： 外部验证模式

本地验证模式

本地验证是一种局部验证模式，是一种点对点的流动性网络。每个节点本身都是一个“路由器”，路由器提供目标链的原始资产，而不是衍生资产。

这种模式的缺点在于无法实现“通用性”，仅仅只能用于资产的跨链传输，而不能用于通用信息和数据的链间传输。

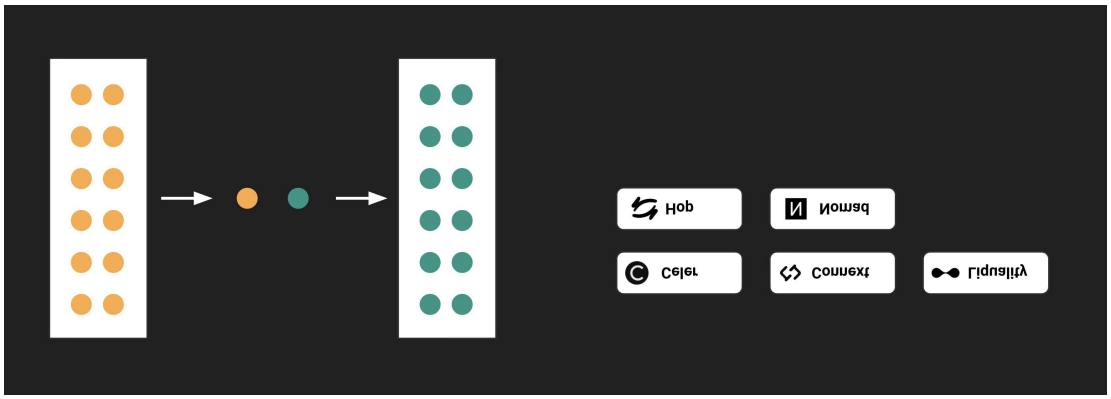

图 3：本地验证模式

上游链模式

上游链要求 dApp 在其链上部署智能合约，这样消息才会被复制并发送到其他 Layer1 公链上以实现状态更新。

该模式的缺点主要体现在商业经营层面，这条链将与所有第 1 层链相互竞争而不是合作，因为彼此都在争夺 dApp 来自己的链上部署。

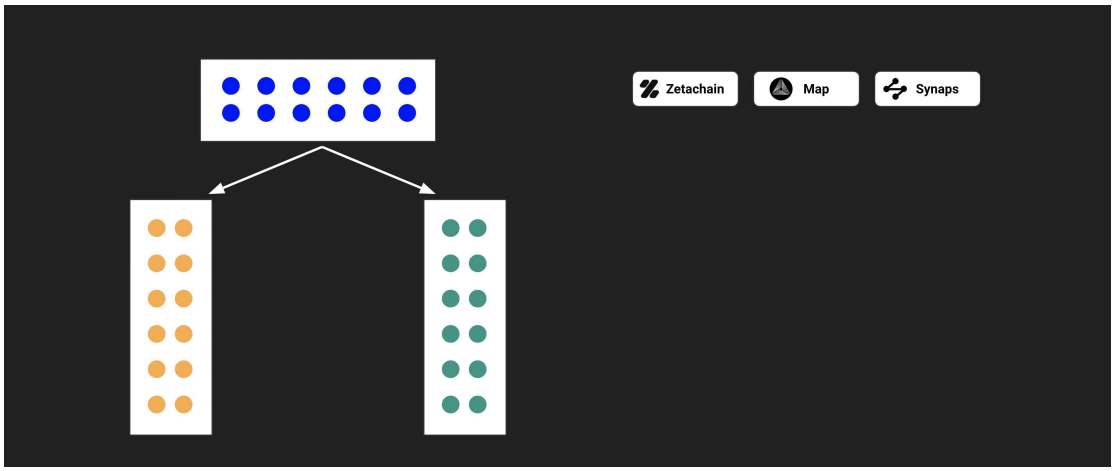

图 4：上游链模式

为什么 zkRelayer 是打开链间通信的钥匙?

一套优秀的链间通信方案应当具备以下优点:

无信任假设，安全，也就是 Trustless, Secure
无许可，去中心化，也就是 Permissionless, Decentralized
通用，也就是 General, Universal
可拓展，也就是 Extensible
快速，低成本，也就是 Efficient, Low Cost

以上优点并不是所有跨链方案都具备，而各个优点的轻重缓急也是不同的。用户可以忍受较慢的跨链服务，也可以忍受较高的跨链成本，也并不一定马上就要做各种数据格式的跨链传输。但是，第一条 Trustless 确实紧迫而重要的。最早的外部验证模式是用一条链去解决其他公链的通信问题，从方法论角度看，它是一种较为笨重的方式，它很难解决在 EVM 和 Non EVM，POW 和 POS 的链间通信难题。与此同时，中间链本身是个单一的中心化工具，且难以“自证清白”，即外部验证模式既没有 Decentralized Security，也没有 Trustless Security。

而原生验证中的 LayerZero 和 Hyperlane 主要强调 Sender 和

Receiver 两个客户端的作用，弱化 Relayer 和 Oracle。这里存在以下几个问题：第一，用户必须相信 Relayer 和 Oracle 不会合谋作恶；第二，用户就必须相信协议本身不会在 Relayer 环节作恶。也就是说，在当前所有解决方案里无法实现 Trustless Security。单点故障和局部故障就像一颗不知道什么时候会爆炸的炸弹，安置在有天然缺陷的跨链通信方案里。

zkRelayer 是 Way Network 提出来的链间通信零知识证明中继器，其优点是用户不需要相信任何外部第三方，也不需要相信协议本身。只要数学和密码学的证明过程完备且正确，这套系统就可以被公众接收。请注意，事情在这里已经发生本质的变化，用户相信的是的”真理”，而不是某人或者某个组织。人或者组织会犯错，会作恶，但真理不会。在整个环节里，Chain A→ Sender→ zkRelayer → ZK Verifier→ Receiver→ Chain B，zkRelayer 的地位将超越 Sender 和 Receiver 这两个轻客户端，成为整套解决方案里的核心。

zkRelayer 的核心部件是 ZK Prover 以及 Message Aggregator。Way Network 的 ZK Prover 所采用的零知识证明方法是 Fox Tech 所提出的 ZK-FOAKS，其优点是非常的快速，且具备 Recursive 和 Trustless 两种特性，其线性证明时间和亚线性验证时间已经达到理论下限。ZK-FOAKS 用在链间通信的 Relayer 之中将确保整个通信是 Trustless，Efficient 且 Low Cost。

zkRelayer 是打开链间通信的钥匙。在 zkRelayer 的加持下，链间通信将掀起新的篇章。