Coinbase Ventures：速览跨链桥现状与趋势

作者：coinbase ventures and Ryan Y Y

翻译：白话区块链



### 1、当前的要点/经验教训

#### 1）分类：桥梁的类型可以划分为三类：本地桥梁、第三方桥梁和桥梁聚合器。

本地桥梁：通常是用户与之交互以存款/提取资产的规范合约。这些可以由一组信任的参与者操作，也可以通过去中心化的共识来操作。运行在兼容的开源堆栈上的链/第二层也可以利用与第一方安全性兼容的桥梁。例如：Optimism OP Stack\*、Arbitrum Nitro\*、Cosmos IBC、Superbridge。

第三方桥梁：是位于链之间并充当“中间人”的网络/验证者。大多数桥梁都采用这种设计的变体。例如：Axelar\*、Wormhole\*、LayerZero (Stargate)\*。

桥梁聚合器：整合上述前两种桥梁，并为最终用户/企业合作伙伴提供跨桥的最佳路径。例如：Socket\*、Li.Fi\*。

#### 2）桥梁的目的

桥梁的主要目的是为数据/资产的（账本/链/位置）与数据/资产的预期执行目的地之间的差值提供服务。主要的用例仍然是资产转移（在一条链上的Token与另一条链上的Token）和交换（在链A上交易Token以获取链B上的Token）。

资产转移：在“链A”上有一种资产（ETH），在“链B”上没有本地发行。桥梁可以为将该资产从“链A”发送到“链B”提供服务。例如，通过 Zora 本地桥\*将 USDC 从 ETH L1 桥接到 Zora L2。

交换：在“链A”上有一笔以（$ETH）换（$ATOM）的交易，在“链B”上有所交易。桥梁将发送Token，然后执行交换。例如：[1] Squid Router“交换”，建立在 Axelar“桥接”之上；[2] 0x的 Matcha\* 负责“交换”，并集成 Socket 来负责“桥接”。

其他：这些可能包括任何类型的调用数据或合约所有权，例如治理或多签所有权。例如，Uniswap v3 合约部署在许多 EVM 链上，但核心治理合约位于 ETH 主网上。Uniswap Foundation\* 宁愿有一个单一的合约，并将消息执行为“一对多”发送到其他链（而不是在每个链上创建治理合约）。

#### 3）桥梁的衡量指标

桥梁通常通过链上AUC（或 TVL）来衡量，作为流动性/使用的指标。

本地桥梁的吸引力直接与 L2 的基础使用密切相关。桥梁合约将持有资金，并可作为衡量资金流向 L2 桥接 TVL 的一种方式。根据 L2 Beat 的数据，Rollups 的 TVL 从约5000万美元到约80亿美元不等。

值得注意的第三方桥梁是基于 TVL、交易量和链覆盖率的拖动力。例如：

LayerZero：TVL：约3.04亿美元；交易量：约239亿美元；交易次数：3450万次。

Wormhole：TVL：约8.5亿美元；交易量：300亿美元；交易次数：170万次。

Axelar：TVL：约2.24亿美元；交易量：70亿美元；交易次数：100万次。

桥梁聚合器通常会路由交易，因此交易量指标更合适。消费者和企业之间的分配（获胜的标志）是关键指标。主要提供商包括 Socket 和 Li.Fi。



#### 4）桥梁的差异化的竞争

桥梁在差异化的各个方面竞争，并且可能会根据一组使用案例和分布情况产生多个赢家。

安全性：安全性细微差异将取决于需求方的偏好。大多数使用桥梁的消费者似乎更喜欢速度/延迟+成本，而不是在最低可行阈值以上的安全性。

智能合约：大多数桥梁的黑客攻击都发生在智能合约层面。在大多数桥梁中，用户将资金锁定在链A的合约中→桥梁读取链A合约→在链B合约中铸造用户的资金。合约中关于提款权限的错误配置可能导致黑客攻击。

多重签名：对合约的控制权被委托给一组信任的参与者。这些通常由项目团队和其他信任的利益相关者操作。

Relayer + Oracle：Dapps / 开发人员可以为其设置自己的转发器 + 预言机。他们也可以从当前可用的转发器 + 预言机设置选项菜单中进行选择。

PoS链：安全性是通过权益证明方式达成的共识。

分布：桥梁将尝试利用现有的合作伙伴渠道，并采取后端基础设施的 GTM。

钱包：桥梁将努力成为现有钱包/投资组合聚合器的桥接功能背后的支撑基础设施/ API。例如，Phantom 与 Li Fi 合作，Coinbase 钱包与 Socket 合作。投资组合前端/钱包将都具有某种形式的桥接支持（例如：Zerion\* / Zapper\* / Metamask\*）。

B2C前端：桥梁通常会建立一个网站门户，任何用户都可以连接钱包+桥接资金。例如：Stargate.Finance（LayerZero）、Bungee.Exchange（Socket）、Jumper.Exchange（Li Fi）和 Squid Router（Axelar）。

Dapps：Dapps 本身将包括一个“存款”功能，该功能在幕后使用桥接，因此用户无需返回 L1，然后再到 L2 使用应用程序。将此视为上面提到的“B2C”的抽象版本，但由开发人员本地支持到应用程序界面。例如：Aevo\*。

开发者平台：许多桥接公司将利用开发者平台的现有分发进行启用。例如：Conduit RaaS、Microsoft Azure + Axelar、Google Cloud + LayerZero。

生态系统：虽然所有主要的第三方桥梁都覆盖了所有相同的链，但它们将努力通过投入资源来在特定链/开发者生态系统中获得先发优势。推理是，随着产品功能集需要更加先进以进行区分，更容易在生态系统的 VM / 智能合约框架内进行扩展。

EVM：Socket 致力于 EVM 滚动升级生态系统（OP Stack、Arbitrum\*、Polygon\* CDK）。Aevo 和 Lyra 等 L2 已是现有用户。

Solana：Wormhole 的生态系统覆盖范围强大，因为他们早期参与其中。DeBridge 也在找到增长的动力。

Cosmos：Axelar 的生态系统覆盖范围强大，因为他们能够提供与 IBC 兼容的交易。一个数据点是利用 IBC 的新链（例如 Celestia\*）在第一天就得到覆盖。

其他生态系统可以由大多数提供商提供服务。

产品/功能集：由于桥梁属于“抽象”业务，它们通常需要进行定制智能合约工作以实现特定的用例。因此，桥梁团队经常会找到专门的垂直/领域，以满足 NFT/支付（例如：Decent）、Gas 抽象和交换等需求。

### 2、我们关注的重点

#### 1）CCTP的作用

CCTP（Circle 的多链 USDC 标准）将是桥梁影响的重要数据点。CCTP 是 Circle 推出的标准，旨在帮助实现 USDC 的多链发行。

CCTP 推出之前：当一个新的链上线时，由于缺乏对本地 USDC 的支持（因为 Circle 必须批准并在其路线图上为每个新链的本地 USDC 添加支持），它会使用桥接版本的 USDC。因为链希望在第一天就能获得 DeFi 支持，所以 USDC 将从 ETH L1 桥接，桥接版本的 USDC 会成为新链上的标准。

例子：一个例子可能是 Axelar 的 axlUSDC 或 Arbitrum 上的 USDC.e - 通过 Axelar 和 Arbitrum 桥梁桥接到 ETH L1 上的 USDC。

影响：这导致了流动性的碎片化，因为链 A 桥接的 USDC 与链 B 桥接的 USDC 对桥梁运营商的依赖性。个别生态系统的 DeFi 协议会将其整合为资产，并且很难解除。

CCTP 推出之后：当一个新的链上线时，它将部署符合 CCTP Circle 标准的 USDC Token合约。当 Circle 准备在链上投入使用时，它可以接管 CCTP 支持的实现。基本上，新的 USDC 合约具有向后兼容性，以符合标准。

例子：NewChain 是一个新的 L2，它上线了，但尚没有本地 USDC。NewChain 部署符合标准的 USDC 合约。NewChain 在短期内支持桥接的 USDC - 但重要的是它可以被 CCTP 接管，并且桥接的 USDC 可以成为本地 USDC。

影响：如果您是开发人员，通常会依赖于桥接的 USDC，并且会被锁定到与资产和桥梁相关的任何流动性计划中。使用 CCTP，您可以过渡到本地启用 USDC，并且可以调用 CCTP API 以启用 USDC 的跨链转移。

#### 2）采用 CCTP 对桥梁的长期防御性产生影响。

桥接的 USDC（非 CCTP）被锁定在 DeFi 池中，并将保持这种状态，直到解除或在链上的资产份额中成为少数。

尽管 CCTP 将与桥梁合作（考虑到它们的分布）以帮助支持 CCTP，但 CCTP 的采用应自然导致本地 USDC 发行的份额增加，桥接的 USDC 的份额减少。在长期内，各种 DeFi 池中锁定的桥接 USDC 资产应自然解除。

例子：桥接到本地 USDC 的比例为：Arbitrum：[57% - 43%]；Base：[33% - 67%]；Optimism：[80% - 20%]；Polygon：[77% - 23%]。

CCTP 的故事将是桥梁的重要经验教训，涉及到接触资产发行方并将其锁定到技术层面的多链优先方法。桥梁将不得不在延迟、安全性和分布等其他差异化领域进行竞争。



只要链的数量和对用户体验抽象化的需求增加，桥梁就会继续发挥作用。

今年，区块空间结算趋势（模块化、Rollups、数据可用性等）的变化将影响用户如何执行交易和移动资产 -桥梁将是实现这种用户体验的热门选择。

随着时间的推移，原生协议和技术的改进应该帮助用户避免提款期限（当前乐观 Rollup 设计中为7天）并实现“快速发送/接收”。

将来，持有链上认证（如 Coinbase 验证）的验证钱包和用户能够在链上与中心化管理的流动性桥梁进行交互。

应用程序托管钱包（和自托管钱包）将继续融入“桥梁增强”工作。在这种情况下，不再将“交换”和“桥梁”作为两个不同的交易，而是将它们合并为一个交易，以获得更好的用户体验结果。

#### 3）桥梁和预言机最终将争夺数据发布的权利

桥梁正在努力赢得第一方发行人利用/使用其基础设施。CCTP 表明，原生发行者希望构建兼容性，减少对任何单一桥梁的依赖性。一些项目正在尝试发行多链的Token标准。尽管 CCTP 专注于 USDC，但Token的本地发行方式可能会有很大不同。例如：OP 在 Optimism 链上本地发行；大多数 ERC20 令牌在 ETH L1 上本地发行。Connext 有一个名为 xERC 的Token标准（类似于任何 ERC20 的 CCTP）。

预言机可以被视为离链数据发布者的“桥梁”。Chainlink 获取离链数据（CeFi 上加密货币的价格）并将其带到链上 - 虽然他们本身并不拥有数据，但通过提供这项服务来实现盈利。从概念上讲，这与桥梁今天的定位类似。预言机和桥梁都将继续为那些需要数据/资产的人和那些可以进行桥接的人之间存在的差值提供服务。最终，它们将需要成为第一方数据发布者的工具，以维护长期的竞争优势/可防御性。Chainlink 拥有自己的桥梁产品CCIP，这进一步证明了它们之间的重叠。

### 3、小结

总之，桥梁和互操作性将继续是大家关注的热门趋势，因为在链的数量不断增长的环境中，为了满足协议和用户对抽象化用户体验的需求，桥梁将成为引人注目的服务提供商。在桥梁景观中，Coinbase Ventures 正在投资于从桥梁中出现的新用例。