BitXHub 白皮书

区块链跨链技术平台

V.1.0.0

杭州趣链科技有限公司

2019年10月

编写成员

顾问：

邱炜伟

研究撰写：

徐才巢、汪小益、夏立伟、陶勇星

统稿：

鲍舒恬

目录

第1章 概述

1.1 跨链背景

当前的区块链底层技术平台百花齐放，但主流区块链平台中的每条链大多仍是一个独立的、垂直的封闭体系。在业务形式日益复杂的商业应用场景下，链与链之间缺乏统一的互联互通机制，这极大限制了区块链技术和应用生态的健康发展，跨链[1]需求由此而来。

跨链指的是通过连接相对独立的区块链系统，实现账本的跨链互操作。跨链交互依据其跨链交互内容的不同可以大体分为资产交换和信息交换。在资产交换方面，一些区块链事实上仍处于互相隔离的状态，它们之间的资产交换主要依靠中心化的交易所来完成，中心化的交换方式既不安全规则也不透明。 而信息交换由于涉及链与链之间的数据同步和相应的跨链调用，实现更为复杂，目前各个区块链应用之间互通壁垒极高，无法有效地进行链上信息共享。

另一方面，区块链技术在单链架构下本身存在着性能、容量不足等问题。单链由于受到目前共识速度的限制，节点的执行性能无法做到线性扩展，这限制了高交易吞吐量低延迟的商业场景的应用。除此之外，随着区块链运行时间的增长，其存储容量也将逐渐增长，且这种数据增长的速度甚至会超过单链存储介质的容量上限。

在业务与技术的双重需求下，链与链之间的互操作得到越来越多的重视，跨链已成区块链技术的必要需求和必然发展趋势。跨链技术作为连接各区块链的桥梁，其主要应用是实现不同区块链之间的资产原子性交易、信息互通、服务互补等功能，以严谨描述、规范实现和普通应用的发展思路，使跨链协议成为“价值互联网”的技术关键。

1.2 产品定义

趣链科技基于链间互操作的需求提出了一种通用的链间消息传输协议，并基于该协议实现了同时支持同构及异构区块链间交易的跨链技术示范平台

BitXHub，允许异构的资产交换、信息互通及服务互补。BitXHub 平台由中继链、应用链以及跨链网关三种角色构成，具有通用跨链传输协议、异构交易验证引擎、多层级路由三大核心功能特性，保证跨链交易的安全性、灵活性与可靠性。

BitXHub 致力于构建一个高可扩展、强鲁棒性、易升级的区块链跨链示范平台，能够为区块链互联网络的形成与价值孤岛的互通提供可靠的底层技术支撑。

第2章 整体架构

2.1 平台架构

为了支持异构区块链之间交易的可信验证和可靠传递，我们设计了一种类似 TCP/IP 的链间传输协议：IBTP（Inter-Blockchain Transfer Protocol）。本平台是一种支持 IBTP 协议的跨链综合服务的参考实现。

如图 2-1 所示是 BitXHub 的整体架构图，BitXHub 平台是一种由中继链、跨链网关和应用链所构建的跨层级链间互操作服务平台。BitXHub 的主要组成部分包括：

- **中继链**（Relay-chain）：中继链用于应用链管理以及跨链交易的可信验证与可靠路由，是一种实现 IBTP 协议的开放许可链；
- **跨链网关**（Pier）：跨链网关担任着区块链间收集和传播交易的角色，既可以支持应用链和中继链之间，也可以支持中继链与中继链之间的交互；
- **应用链**（App-chain）：应用链负责具体的业务逻辑，分为：1）同构应用链（支持 IBTP 协议的区块链），具有类似的区块结构和交易数据存储格式，并具有相同的共识算法[2]和加密机制等，如趣链联盟链平台。2）异构应用链，是指不直接支持 IBTP 协议的区块链，例如 Fabric[3]、以太坊[4]等。

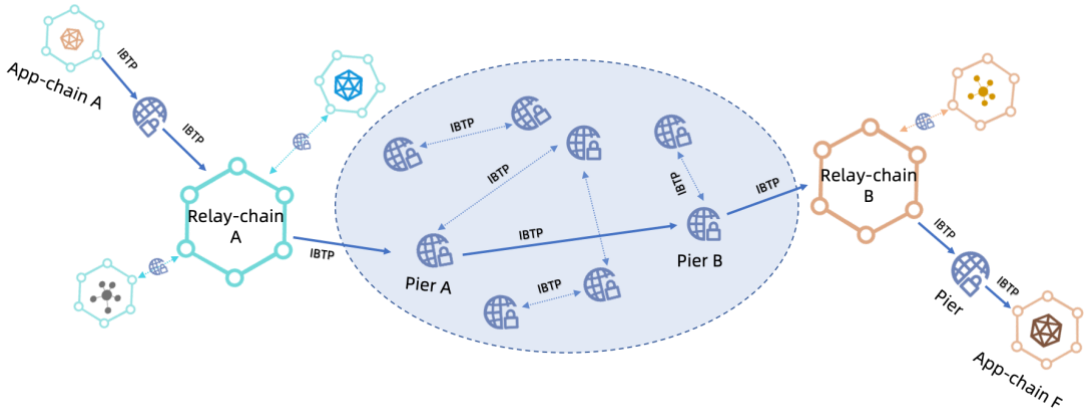

图 2-1 BitXHub 架构图

2.2 核心流程

由于单个中继链的处理能力有限，我们假设每个中继链支持不超过 64 个应用链的跨链管理，具体应用链的个数根据跨链业务的复杂度进行动态调整。因此在整个跨链生态中必然会出现多个以中继链为中心的区块链联盟，那么跨链交易如何在整个跨链生态中进行流转呢？如图 2-2 所示为 BitXHub 中交易处理的核心流程：

1. 应用链 1 发起跨链交易，记为 ct1;

2. 跨链交易 ct1 被提交到应用链 1 所关联的中继链 A;

3. 中继链 A 验证跨链交易 ct1 是否可信，一是验证交易来源的可信，二是验证交易证明是否满足应用链对应的规则；

   3.1 如果验证不通过，则执行步骤 4；

   3.2 如果通过，则执行步骤 5；

4. 非法交易回滚，执行步骤 11；

5. 中继链 A 判断 ct1 的目的链是否在其管理的应用链列表中，如果存在则执行步骤 6，否则执行步骤 7；

6. 提交 ct1 到目的链；执行步骤 11；

7. 提交 ct1 到中继链 A 相关联的跨链网关 1；

8. 跨链网关 1 根据 ct1 的目的链地址，在跨链网关集群中通过分布式哈希表的方式进行查询，如果目的链所关联的中继链 B 的跨链网关 2 存在则执行步骤 9，否则执行步骤 4；

9. 跨链网关 1 将 ct1 发送给跨链网关 2，跨链网关 2 将其提交到目的链所关联的中继链 B;

10. 中继链 B 验证 ct1 是否通过前置中继链（即中继链 A）的验证背书；如果背书验证可信则执行步骤 6；否则执行步骤 4；

11. 结束交易。

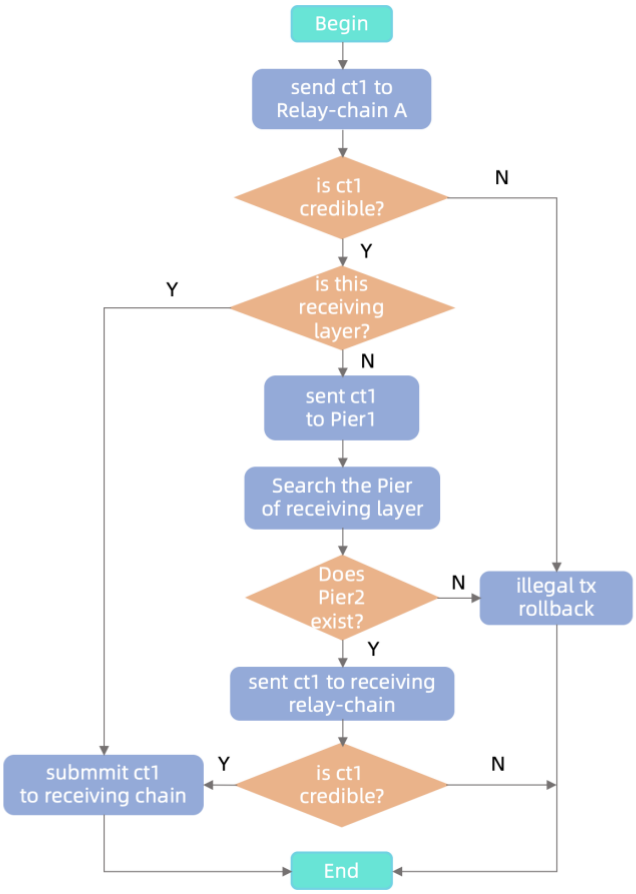

图 2-2 BitXHub 交易处理核心流程

第3章 IBTP 协议

异构应用链间共识算法、加密机制等的不同会导致交易合法性证明各不相同。为了中继链更方便地进行跨链消息的验证和路由以及跨链网关更一致地进行跨链消息处理，BitXHub 设计了一种类似 TCP/IP 的通用链间消息传输协议。

3.1 结构说明

IBTP 为了通用性和灵活性设置了一些主要的数据字段，具体如表 3-1 所示：

表 3-1 IBTP 协议数据结构

参数	说明
From	来源链 ID
To	目的链 ID
Version	协议版本号
Index	跨链交易索引
Payload	跨链调用内容编码
Timestamp	跨链事件发生的时间戳
Proof	跨链交易证明
Extra	自定义字段

其中 From 和 To 字段分别代表来源链和目的链的 ID，ID 在应用链向中继链注册时生成。Index 是跨链交易的索引，它是中继链顺序打包跨链交易的依据，跨链交易按其来源链 ID 分别进行排序编码。Version 字段标识了 IBTP 的版本信息。

Payload 字段是跨链调用的内容编码，支持定向加密，可由应用链的业务需求确定。Timestamp 字段是跨链交易的一个时间标识。

Proof 字段存储了跨链交易合法性证明，为中继链跨链验证引擎提供具体的验证信息。Proof 字段内容根据来源链的不同而不同，具体验证规则可通过动态加载的方式注册到跨链验证引擎。

最后，IBTP 协议提供了一个扩展字段 Extra，根据应用链的业务需求进行自

定义。

3.2 跨链消息证明

应用链的异构与否导致的 IBTP 结构差异主要体现在 Proof 字段上。Proof 是跨链交易合法性的一个凭证，下面从异构应用链和同构应用链两个角度去详细阐述 IBTP 结构的构建。

3.2.1 同构应用链

下面以同构应用链为例简单说明 IBTP 的构造过程。其中，跨链交易组成的 Merkle Tree 结构[5]可以参见 4.1 节。

同构应用链所构建的 IBTP 结构如图 3-1 所示：

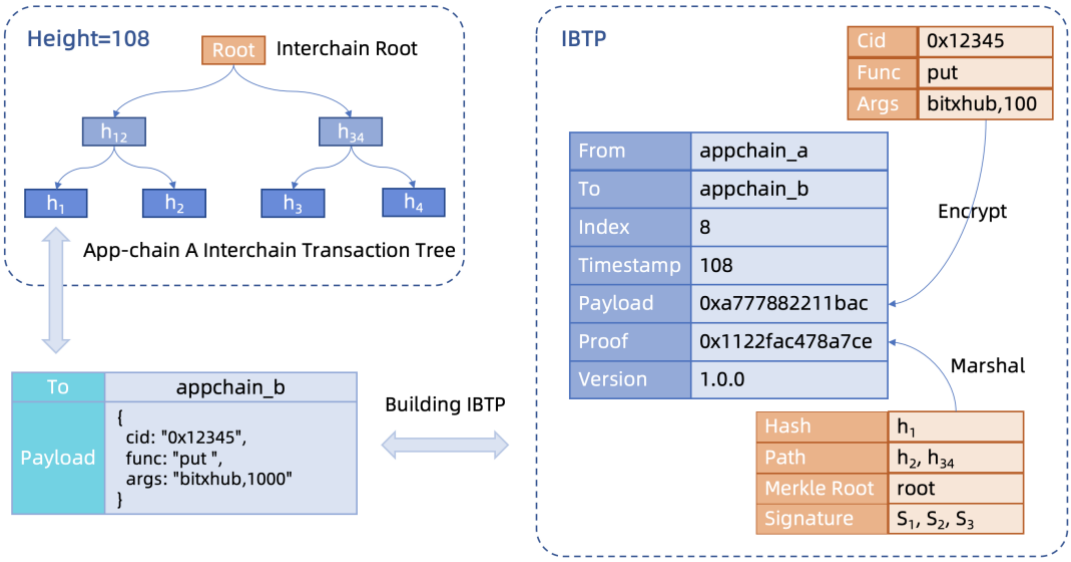

图 3-1 同构应用链构建的 IBTP 结构

以 108 号区块的第一个跨链交易为例，对于应用链 B 中地址为“0x12345”的合约，该交易调用合约方法“put”，参数为“bitxhub, 1000”。Proof 提供 Merkle 路径的信息，其中 Hash 是跨链交易相关内容的哈希，Path 是 SPV 路径哈希，MerkleRoot 是最终的根哈希，Signature 是对于根哈希的签名。

3.2.2 异构应用链

异构应用链分为两种，一种是及时确认并且交易本身有验证节点作为背书的区块链，比如 Fabric 等；另一种是概率确认性质或者交易本身没有验证节点的区

块链，比如比特币[6]、以太坊等。

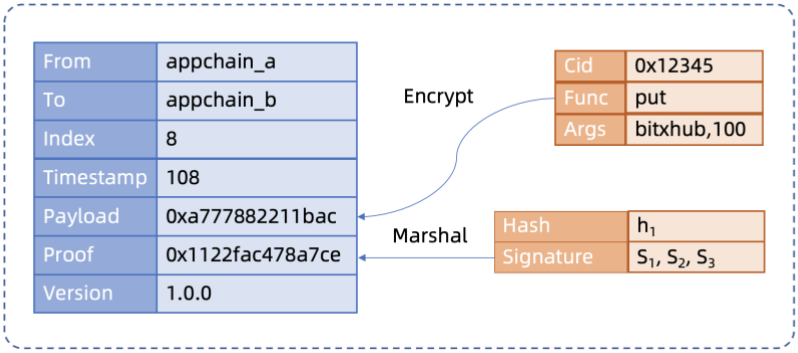

图 3-2 异构应用链构建的 IBTP 结构

第一种类型的异构应用链已满足 IBTP 协议的构造条件，因此跨链网关只需要调用应用链的 SDK 即可实现 IBTP 的构建。图 3-2 是以 Fabric 为应用链的 IBTP 结构。其中 Proof 字段包含的 Hash 字段是 Fabric 中 chaincode 执行结果的摘要，Signature 字段则是背书节点对 Hash 字段的签名数组。而对应的背书节点的证书信息已经在应用链注册时登记到中继链中[7]。

第二种类型以以太坊为例，其本身是概率性确认的区块链，且抛出的跨链事件未携带签名信息。因此跨链交易合法性证明需要由多个跨链网关协作构造，跨链网关的可靠性通过激励和惩罚机制进行保证。

第4章 中继链

中继链用于应用链的跨链管理，以及跨链交易的可信验证与可靠路由，是一种实现 IBTP 协议的开放许可链，中继链与中继链间还可进一步实现跨链交易证明的跨层级信任传递[8]。

4.1 关键存储结构

中继链本身需要提供跨链交易的合法性证明，所以其存储结构比传统区块链多了一个由跨链交易构成的 Merkle Tree。中继链的 Merkle Tree 构造如图 4-1 所示，每个区块中的跨链交易组成一个新的 Merkle Tree，其中叶子节点是跨链交易的哈希，它的 Merkle Root 和传统区块的 Merkle Root 再算出一个新的 Merkle Root。验证者会对最终的 Merkle Root 进行签名。

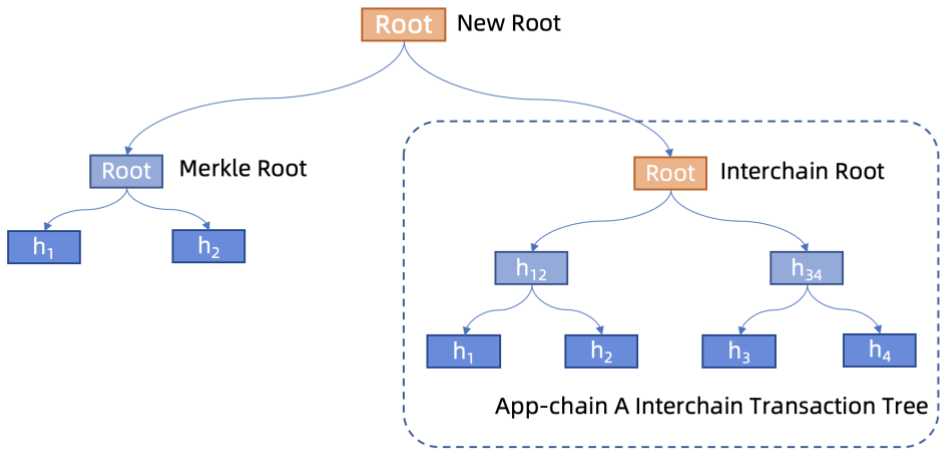

图 4-1 中继链存储结构示意图

4.2 验证引擎

我们为中继链设计了一种高效可插拔的验证引擎，用于支持应用链所提交的跨链交易可信验证，基于动态注入的验证规则对相应应用链提交的证明进行验证.

在应用链接入之前，首先需要进行验证规则的编写和注册，由中继链审核后才能部署到验证引擎。

在跨链交易中，对于每一笔跨链交易，中继链需要对其进行校验，防止交易被伪造或篡改。验证引擎通过智能合约的方式管理多种验证规则，对不同区块链

的交易进行合法性检验，并支持验证规则的在线升级和改造。

验证引擎的工作流程主要分为以下三个步骤：

- **协议解析**是验证引擎内部对跨链交易的解析。由于所有跨链交易都遵循 IBTP 协议，通过该步骤可以解析出交易的来源链信息和验证证明信息作为后续验证引擎的输入。
- **规则匹配**是验证引擎根据上述步骤解析出的来源链类型去匹配对应的验证规则脚本。
- **规则执行**是验证引擎的核心，主要通过 WASM 虚拟机[9]动态加载规则脚本，然后对跨链交易的 Proof 字段进行校验，从而确定交易的合法性。

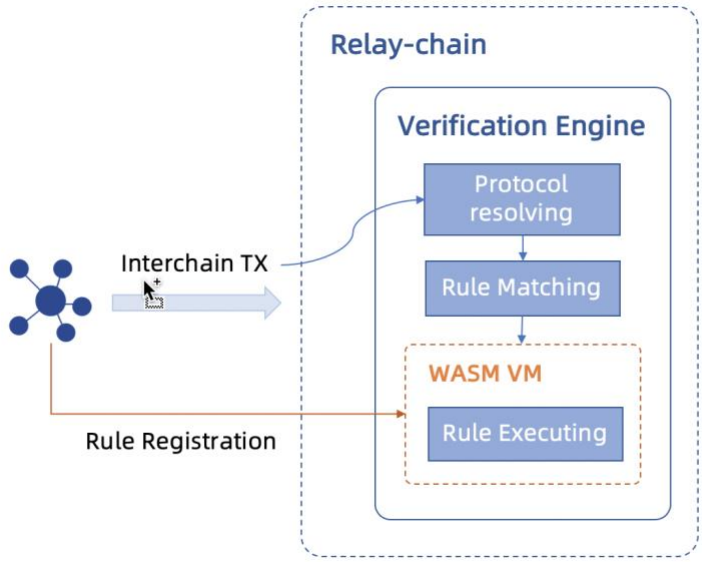

图 4-2 中继链交易验证流程示意图

综上所述，中继链的异构交易验证引擎具有诸多优势：

- 高效：通过 WASM 虚拟机保证了验证规则的执行的高效性。
- 更新：验证规则依据不同区块链的规则的变化快速、低成本的热更新。
- 全面：满足各类型区块链的验证体系。
- 便捷：应用链的业务人员可以直接管理验证脚本中的校验规则。
- 安全：对 WASM 虚拟机设置安全限制，只能调用引擎自身所允许的函数和库。

4.3 交易路由

中继链除了需要对跨链交易的合法性进行验证，同时还肩负着跨链交易路由的职责。路由对象包括两个方面：一是跨链交易，二是具有回调的跨链交易回执。

一个区块中所有要被路由的跨链交易会被构建成如图 4-3 所示的 Merkle Tree，其中 Merkle Root 会经过验证节点的签名。（AC1 代表的是从 A 发到 C 的 1 号跨链交易）

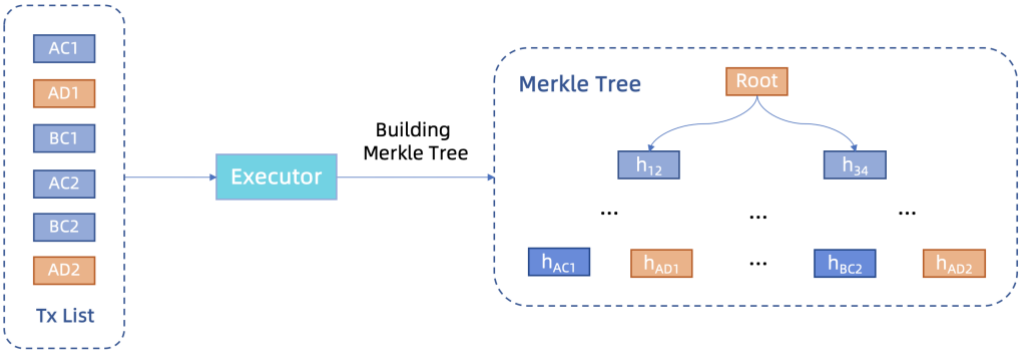

图 4-3 跨链交易路由

中继链执行完一个区块后会根据目的链 ID 进行交易分类，如图 4-4 所示路由模块根据 C 和 D 两个目的链把跨链交易分成两部分。Pier C 和 Pier D 会从中继链同步与自己相关的跨链交易和跨链交易证明。如果跨链交易是跨层级的，Pier 还需添加该条跨链交易来自中继链的证明信息，以供目的中继链进行验证。

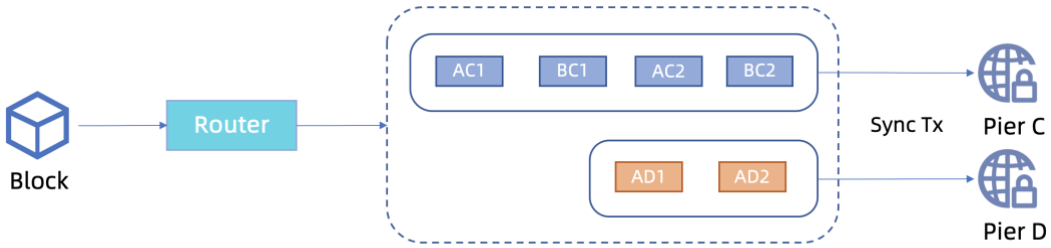

图 4-4 跨链交易分类与执行

跨链网关 Pier 对于不同来源链的交易可以并行执行。执行完的回执分为两种，一种是没有回调的跨链交易对应的回执，在返回中继链后完成跨链。另一种是有回调的跨链交易对应的回执，经过中继链的排序打包后返回来源链。

第5章 跨链网关

在复杂的跨链场景下，应用链如何便捷地接入跨链系统以达到良好的扩展性，对于激发跨链系统生态的活力至关重要。跨链网关 Pier 是一个能够满足应用链接入便捷性和多层级扩展性的一个关键接入口。

本质上来说，Pier 是一种连接不同区块链系统的交互组件，在 BitXHub 中充当着两个不同的角色：

- 连接应用链和中继链。在单中继链的层级中，Pier 作为一个中间部件来简化区块链接入跨链系统的过程，增强接入跨链系统的便捷性。
- 连接不同的中继链。在多中继链形成的区块链网络中，Pier 通过 P2P 组网的方式在多个层级中起到“路由器”的作用。

为了实现上述的便捷性和可扩展性，Pier 在应用链的适配和核心功能的实现上作了灵活设计。

5.1 插件机制

现有的区块链平台在架构设计上存在着较大的差异，如何将其快速、便捷地接入跨链系统是一个亟待解决的问题。

插件机制的一大特点是将 Pier 中与应用链的交互模块和核心模块进行解耦，从而方便更多的应用链加入跨链系统。在 Pier 运行时，通过动态加载插件的方式完成应用链的接入。为了提升与应用链的交互能力，插件需要根据不同区块链的特性实现具体的接口，交互接口需要满足以下几个功能：

- 监听相应区块链上的跨链事件并传给核心模块进行处理；
- 执行来自于其他区块链的跨链请求；
- 能够查询相应区块链上已收到和已执行的跨链请求状态。

在插件机制下，Pier 具有如下两点优势：

- 易接入，便于适配不同的区块链，无需对 Pier 核心模块进行改动；
- 热更新，可在 Pier 不停机的情况下动态更新插件。

5.2 核心模块

5.2.1 跨链交易收集

Pier 在对接具体的应用链时，不仅要监听交易，而且需要保证跨链交易的有序性和可验证性。为此，Pier 需要拥有应用链一定的权限，例如收集 Fabric 跨链交易时，需要有权限获取背书信息。

由于应用链的不同，Pier 收集跨链交易的策略也应视情况而制定。下面以同构应用链和异构应用链两个角度进行分析。

对于同构应用链，Pier 在监听到跨链事件后，只需要根据区块存储结构获取该跨链消息的合法性证明，即可构造 IBTP 结构。

对于异构应用链，以以太坊为例进行分析。以太坊采用基于概率性确认的 PoW[10]共识机制，所以 Pier 收集到一个跨链交易时，并不能立即确认其是否为有效交易。在这种情况下，Pier 需要设定一个等待阈值（一般为 20 个区块后），使得该跨链交易有极大概率被确认后，再将其转发到中继链。

考虑到单个 Pier 可能产生恶意行为，如谎称交易已经确认等，需要采用 Pier 集群的方式来增强跨链网关的可信度。如图 5-1 所示，每个 Pier 由权威机构进行背书，并在中继链上引入对作恶网关的惩罚机制，通过经济激励的方式防止多个 Pier 联合作恶。另外以太坊本身对未对跨链交易签名，所以需要多个 Pier 确认跨链交易的存在并对其进行签名，然后转发到中继链上。

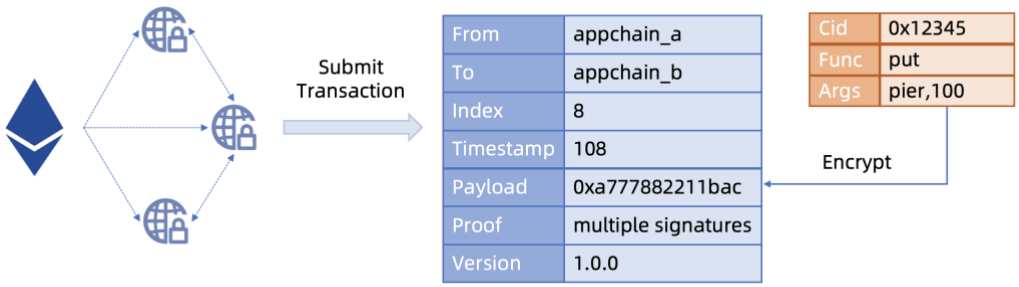

图 5-1 公链跨链交易构建

5.2.2 同步与执行

Pier 提交跨链交易之后，中继链会对跨链交易进行打包。各个 Pier 节点会自动同步中继链上的跨链交易并通过合法性证明确认跨链交易的可信。

之后，Pier 使用与交易来源方协商的对称密钥解析跨链交易，得到具体的 IBTP 结构，并构造出跨链事件。Pier 根据具体应用链的特定规则，选择相应的插件处理。

5.3 跨链路由网络

在多层级区块链网络中，需要跨链路由网络进行跨链交易的传递。跨链路由网络是一个由多个 Pier 组成的 P2P 网络。

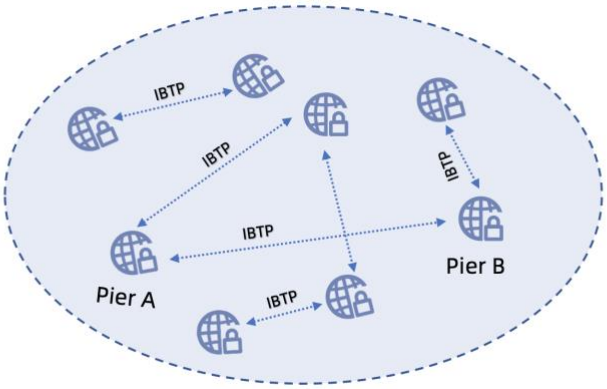

图 5-2 跨链路由网络拓扑图

每个 Pier 会维护一个全网的路由表，记录应用链和中继链的关联关系。Pier 在加入路由网络时，需要广播所属中继链管理的所有应用链信息，其他 Pier 会根据广播信息进行路由表的更新。

当 Pier 传递跨链交易时，首先通过路由算法查找跨链交易的目的中继链对应的 Pier，并通过跨链路由网络进行传输。目的 Pier 验证跨链交易来源的真实性，通过验证后再将跨链交易发送到相应的中继链。跨链交易的执行结果也通过该方式将执行结果返回来源中继链[11]。

第6章 总结与展望

BitXHub 为公链和联盟链提供了一套自主创新、透明可信的跨链技术方案，基于通用跨链消息传输协议 IBTP 打造了一个异构区块链跨链示范平台，秉承着去中心、可扩展、高可用、易接入的设计理念，为链上的资产、数据、服务开拓价值互通的渠道，助力区块链技术从“链孤岛”到形成“链网络”的发展。

跨链技术的生命力来自于所有区块链技术人员与相关行业从业者，因此 BitXHub 希望开放一种跨链通用协议，为跨链平台增添一份公信力，希望构建一个自由、活跃、先进的开源社区以丰富与完善跨链标准，能够桥接更多类型各异的区块链平台，与多方共同探索跨链的生态系统，共创跨链的深远价值。

参考文献

[1] Buterin, Vitalik. "Chain interoperability." R3 Research Paper (2016).

[2] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance." OSDI. Vol. 99. No. 1999. 1999.

[3] Cachin, Christian. "Architecture of the hyperledger blockchain fabric." Workshop on distributed cryptocurrencies and consensus ledgers. Vol. 310. 2016.

[4] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151.2014 (2014): 1-32.

[5] Szydlo, Michael. "Merkle tree traversal in log space and time." International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2004.

[6] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[7] Fabric docs: https://hyperledger-fabric.readthedocs.io/en/release-1.4/txflow.html

[8] Kan, Luo, et al. "A multiple blockchains architecture on inter-blockchain communication." 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). IEEE, 2018.

[9] Haas, Andreas, et al. "Bringing the web up to speed with WebAssembly." ACM SIGPLAN Notices. Vol. 52. No. 6. ACM, 2017.

[10] Chen, Zhi-dong, et al. "Inter-blockchain communication." DEStech Transactions on Computer Science and Engineering cst (2017).

[11] Gervais, Arthur, et al. "On the security and performance of proof of work blockchains." Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. ACM, 2016.