区块链跨链技术调研分析与对比评估

南京大学

软件学院

SP & DevOps 实验室

Version 1.0

2020 年 09 月 14 日

文档版本控制记录：

版本号	版本更改说明	更改人员	更改日期
0.1	完成报告主体部分	胥倩雯，王岩泽等	2020.08.01
0.2	完成初稿	胥倩雯，王岩泽等	2020.08.06
0.3	完善引用	王岩泽，胥倩雯	2020.08.07
0.4	增加各章小节	胥倩雯	2020.08.07
0.5	结构调整，增加表目录	胥倩雯	2020.08.08
0.6	格式调整，内容补充润色	王岩泽	2020.08.09
0.7	审阅，部分内容修改润色	李杉杉、胥倩雯、王岩泽	2020.08.13
0.8	审阅，1、2章节修改润色	李杉杉	2020.08.26
0.9	根据意见修改和完善	胥倩雯，王岩泽	2020.08.30
1.0	3、4、5章节修改润色	李杉杉	2020.09.14

摘 要

随着区块链发展进入3.0时代，区块链技术逐渐成熟完善，应用范围进一步拓宽，各种场景下的落地项目也不断成熟。区块链技术改变了传统的信任模式，为人类社会的金融贸易带来了新的技术变革。然而，链与链之间存在严重的信息沟壑，区块链的封闭性和独立性导致区块链之间形成大量的数据孤岛，信息孤立成为了制约区块链技术广泛应用的重要因素之一。随着多样化、复杂化的区块链系统不断完善，孤岛现象日趋严峻，使得解决区块链间的互操作性以实现跨链信息互通与资产流动成为极具挑战性并且亟待解决的问题。

跨链技术是应对区块链互操作性需求的关键，但该技术目前仍然处于发展起步阶段。为此，本文开展了针对跨链技术解决方案的调研研究，通过对已有的区块链跨链技术实现思路、特点及挑战问题进行系统化分析，旨在帮助了解区块链技术的发展现状和发掘未来关于该技术的研究方向。本文检索得到了103个跨链技术解决方案对应的学术文献或灰色文献（技术报告、白皮书等），通过初步分析，得到了 5 个主流跨链机制下的分类结果，并给出了关于现状的总体描述；本文进而选择了不同分类下的 22 个典型方案进行详细研究，并对比评估了每个分类下的解决方案；最后，本文对不同分类下的解决方法进行横向对比，综合分析了区块链跨链技术发展过程中的技术难点与挑战性问题，如安全性、可扩展性和性能等，并给出了关于未来研究方向的建议。

关键词：区块链；跨链技术；互操作性；调研；挑战

目 录

第 1 章 引言 - 1 -
1.1 背景概述 - 1 -
1.2 国内外研究现状 - 1 -
1.3 研究目的、研究方法及贡献 - 2 -
1.3.1 研究目的 - 2 -
1.3.2 研究方法及贡献 - 3 -
1.4 本文组织结构 - 3 -
第 2 章 基本概念及研究方法 - 5 -
2.1 区块链概述 - 5 -
2.1.1 区块链类型 - 5 -
2.1.2 区块链架构与模型 - 5 -
2.2 主流区块链底层技术平台 - 8 -
2.2.1 Bitcoin - 8 -
2.2.2 Ethereum - 8 -
2.2.3 EOS - 8 -
2.2.4 Hyperledger 系列 - 9 -
2.2.5 Multichain - 9 -
2.2.6 比较 - 9 -
2.3 区块链跨链技术 - 10 -
2.3.1 概念 - 10 -
2.3.2 基本原理 - 11 -
2.3.3 跨链机制 - 12 -
2.4 本章小结 - 15 -
第 3 章 现有跨链技术对比分析 - 16 -
3.1 侧链/中继机制 - 17 -
3.1.1 总体概述 - 17 -
3.1.2 基于侧链/中继机制的典型跨链解决方案 - 18 -
3.1.3 总结 - 24 -
3.2 公证人机制 - 24 -
3.2.1 总体概述 - 24 -
3.2.2 基于公证人机制的典型跨链解决方案 - 24 -
3.2.3 总结 - 30 -
3.3 哈希锁定机制 - 30 -

3.3.1 总体概述 - 30 -
3.3.2 基于哈希锁定的典型跨链解决方案 - 30 -
3.3.3 总结 - 34 -
3.4 区块链分片机制 - 34 -
3.4.1 总体概述 - 34 -
3.4.2 基于区块链分片的典型跨链解决方案 - 35 -
3.4.3 总结 - 40 -
3.5 分布式私钥控制机制 - 40 -
3.5.1 总体概述 - 40 -
3.5.2 基于分布式私钥控制机制的典型跨链解决方案 - 41 -
3.5.3 总结 - 44 -
3.6 其他跨链机制 - 45 -
3.6.1 总体概述 - 45 -
3.6.2 其他跨链机制的典型跨链解决方案 - 45 -
3.7 本章小结 - 49 -
第 4 章 进一步讨论 - 50 -
4.1 跨链机制间对比分析 - 50 -
4.1.1 技术性对比 - 50 -
4.1.2 非技术性对比 - 51 -
4.2 跨链技术难点与解决方案 - 53 -
4.3 本章小结 - 57 -
第 5 章 总结展望 - 58 -
参考文献 - 60 -

图目录

图 2-1： 区块链的基础架构模型 - 6 -
图 2-2： 跨链层级架构图 - 11 -
图 3-1： 现有跨链技术解决方案所依据的跨链机制分类情况 - 16 -
图 3-2： 项目发布时间分布图 - 16 -
图 3-3： 跨链两侧支持的区块链 - 17 -
图 3-4： 侧链/中继的跨链解决方案图 - 18 -
图 3-5： 公证人机制的跨链解决方案图 - 24 -
图 3-6： 哈希锁定的跨链解决方案图 - 30 -
图 3-7： 区块链分片的跨链解决方案图 - 35 -

图 3-8 ： 分布式私钥控制的跨链解决方案图 ..... - 41 -
图 4-1 ： 各技术难点数量统计 ..... - 53 -

表目录

表 2-1 区块链平台技术对比 ..... - 9 -
表 2-2 区块链平台交易行情对比 ..... - 9 -
表 3-1 基于侧链/中继的项目间平台、跨链类型、消息验证等对比 ..... - 20 -
表 3-2 基于侧链/中继的项目间通讯协议对比 ..... - 21 -
表 3-3 基于侧链/中继的项目间共识机制对比 ..... - 22 -
表 3-4 基于侧链/中继的项目间应用场景对比 ..... - 22 -
表 3-5 基于侧链/中继的项目间特性对比 ..... - 23 -
表 3-6 基于侧链/中继的项目间限制对比 ..... - 23 -
表 3-7 基于公证人的项目间平台、跨链类型、消息验证等对比 ..... - 27 -
表 3-8 基于公证人的项目间通讯协议对比 ..... - 27 -
表 3-9 基于公证人的项目间共识机制对比 ..... - 28 -
表 3-10 基于公证人的项目间应用场景对比 ..... - 28 -
表 3-11 基于公证人的项目间特性对比 ..... - 29 -
表 3-12 基于公证人的项目间限制对比 ..... - 29 -
表 3-13 基于哈希锁定的项目间平台、跨链类型、消息验证对比 ..... - 32 -
表 3-14 基于哈希锁定的项目间通讯协议对比 ..... - 32 -
表 3-15 基于哈希锁定的项目间共识机制对比 ..... - 32 -
表 3-16 基于哈希锁定的项目间应用场景对比 ..... - 33 -
表 3-17 基于哈希锁定的项目间特性对比 ..... - 33 -
表 3-18 基于哈希锁定的项目间限制对比 ..... - 34 -
表 3-19 基于分片的项目间平台、跨链类型、消息验证对比 ..... - 38 -
表 3-20 基于分片的项目间通讯协议对比 ..... - 38 -
表 3-21 基于分片的项目间共识机制对比 ..... - 39 -
表 3-22 基于分片的项目间应用场景对比 ..... - 39 -
表 3-23 基于分片的项目间限制对比 ..... - 40 -
表 3-24 基于分布式私钥控制的项目间平台、跨链类型、消息验证对比 - 42 -
表 3-25 基于分布式私钥控制的项目间通讯协议对比 ..... - 42 -
表 3-26 基于分布式私钥控制的项目间共识机制对比 ..... - 43 -
表 3-27 基于分布式私钥控制的项目间应用场景对比 ..... - 43 -
表 3-28 基于分布式私钥控制的项目间特性对比 ..... - 44 -

表 3-29 基于分布式私钥控制的项目间限制对比 - 44 -
表 3-30 项目间目的/着眼点对比 - 46 -
表 3-31 项目间平台、跨链类型、消息验证对比 - 47 -
表 3-32 项目间通讯协议对比 - 47 -
表 3-33 项目间共识机制对比 - 48 -
表 3-34 项目间应用场景对比 - 48 -
表 3-35 项目间特性对比 - 48 -
表 3-36 项目间限制对比 - 49 -
表 4-1 跨链机制间技术对比 - 50 -
表 4-2 跨链机制间优缺点对比 - 51 -

第1章 引言

1.1 背景概述

中本聪在 2009 年发布比特币白皮书[1]，开启人们对区块链这一比特币背后技术的研究。区块链是一个不断增长的记录列表，采用了密码学技术，具有去中心化、不可变、防篡改等性质，可以在没有第三方中介的情况下通过互联网实现资产、信息的安全转移。现如今，区块链已扩展到金融以外的多个领域，包括物联网、智能制造、医疗、供应链、身份管理等。区块链项目的数量正呈爆炸式增长，越来越多的开发人员尝试利用这一新技术，跳出原有的思维模式，建立去中心化网络应用。

随着区块链技术快速发展，出现了许多不同种类的区块链，它们执行不同的交易，处理不同大小的数据，或是为特定的工会、社区组织和政府部门设计。但是，由于不同区块链使用不同的协议与技术，它们之间无法交换代币（Token），也不能交换状态或事件信息，导致了不同区块链之间形成隔离。例如，建立在以太坊上的项目可以轻松地与以太坊平台上建立的其他项目进行交互，但是不能与 EOS[2]，TRON[3]或其他智能合约平台上建立的项目进行交互。智能合约平台是封闭式的，禁止与特定环境之外的任何项目共享数据或价值。

当今的数字经济要求多个系统相互通信，IBM 研究员兼区块链技术副总裁 Jerry Cuomo 指出，“数字系统的互操作性很重要，区块链是数字系统的最新和最大突破，因此它也同样适用”。跨链技术能够克服区块链的局限性，并且将区块链从这种分散的孤岛中解救出来，是扩展和连接区块链的桥梁[4]**错误!未找到引用源。**。

跨链意味着无需中间人即可跨不同网络共享、查看和访问信息，或者依据另一个区块链的状态更改进行操作。用户可以从跨链互操作中受益，通过连接多个较小的区块链可以提高区块链的性能，通过在另一个区块链上提供一种备份可以减小区块链不可用或受到攻击的风险[5]。同时，跨链也对区块链提出了一些技术要求（例如，验证机制等）和非技术要求（例如，安全性等），因此开发人员需仔细比较跨链方案，选择最合适其项目的方案。目前为止，跨链已经有了很多理论和实践经验。

1.2 国内外研究现状

在区块链跨链技术调研方面上前人做了大量的工作，通过对当下跨链的重要性以及主流跨链技术类型与特性进行精准总结与归纳，为本次研究工作提供充实的信息与可靠数据来源。

2018 年，李芳等人[6]针对目前区块链价值孤岛现象，分析了跨链技术的必要性、难点，同时对已有跨链技术进行介绍总结并列举了 12 种安全性风险。Jin 等人[7]对于实现区块链系统间的跨链交互进行研究，针对跨链技术的理论与实践方面的挑战进行了分析。Deng 等人[8]介绍了跨链技术与多签名钱包的原理与案例，对当下主流跨链机制与跨链项目加以讨论。2019 年，Hegnauer[9]分析了现有跨链解决方案与研究现状，提出互操作性的重要性，特别是侧链最具发展前景。Mahdi 等人[10]指出数字加密货币贸易缺乏互操作性与可伸缩性，并对原子交换技术的应用项目与市场发展展开调查，并分析其优势与挑战。之后，路爱同等人[11]分析了跨链技术特性、难点与参考解决方案，并对四种跨链机制进行介绍和对比。2020 年，Kannengießer 等人[12]在研究中对理论与实践中的跨链技术加以整合，提出对跨链技术的全面见解。Qasse 等人[13]则通过不同角度对已有的跨链解决方案进行调研分析，将跨链项目归纳为侧链、区块链路由、智能合约、工业解决方案（Industrial Solution）四类，讨论比较架构之间的特性。Robinson[14]调研目前主流的跨链机制的同时，重点研究了跨链共识的重要性以及跨链共识针对不同类型区块链的应用方式。2020 年 3 月，区块链服务网络发展联盟发布了区块链服务网络用户手册，手册中提到区块链服务网络 BSN 的愿景是成为区块链互联网，跨链是 BSN 技术体系内非常核心的一部分[15]。2020 年 7 月，中国信息通信研究院牵头编写区块链互操作白皮书[16]，从应用层互操作、链间互操作和链下数据互操作三个方面对跨链互操作性进行讨论，分析了不同方面下的需求现状，并给出了发展建议。

对于跨链机制与跨链项目已经存在大量的相关讨论，学者们或从不同角度分类，或从不同切入点研究，对已有技术加以分析并对未来进行展望。但目前尚未有研究对现有的跨链项目进行全面整合分析。

1.3 研究目的、研究方法及贡献

1.3.1 研究目的

为了探究跨链技术的实践经验和存在的挑战，我们设计了三个主要的研究问题：

•**研究问题 1**：目前存在哪些跨链技术的解决方案用以解决区块链的互操作性需求？

•**研究问题 2**：所探究的跨链技术方案如何应对区块链的互操作性需求？

•**研究问题 3**：所探究的跨链技术解决方案目前存在哪些挑战以及如何应对？

研究问题 1 旨在调研跨链技术解决方案在学术界和工业界的发展现状，提供关于该技术的全景介绍和分类情况；**研究问题 2** 的回答是为了深入分析现有

跨链技术解决方案的实现机制、相同和不同跨链机制分类下的特点等；**研究问题 3 的目的**在于发现跨链技术的难点问题，尤其是发掘攻克难点问题可能的思路，以此驱动未来进一步的研究和探索。

1.3.2 研究方法及贡献

本文通过普通学术文献加灰色文献检索相结合的方式系统化收集数据，最后得到了 103 项不同成熟度的、用以解决区块链互操作性的跨链技术解决方案。本文首先按照通用的跨链机制标准对检索到的方案进行分类，并详细探究了每个范畴下最典型且成熟的解决方案项目。之后通过对已有跨链综述或二级研究的分析以及对各个项目白皮书、官网介绍等共性内容的提取，总结出应用环境、共识机制、验证机制、通信协议等方面内容。通过进行全面对比，体现各个项目特性并比较其优势和劣势，分析出不同跨链机制下的技术考量点与适用场景。在此之上，本文进一步整合分析了不同跨链机制下的方案信息，并进行机制间方案的横向对比，归纳出区块链平台开发时普遍会关注的性能要点、项目常见的技术难点以及未来可考虑的研究方向。

本文的贡献主要包括以下三点：

1）探究应对区块链互操作需求的跨链技术解决方案的集合，帮助学术界和工业界建立对跨链技术发展现状的基本理解；

2）分析当前跨链技术解决方案的实现思路和基本原理，对比相同和不同原理分类下技术的特点，为进一步探究并解决区块链的互操作性问题奠定理论基础；

3）发掘当前跨链技术解决方案的痛点问题和面临的挑战，为未来学术领域的研究指明可能的研究方向，一定程度上帮助推进区块链跨链技术理论的发展。

1.4 本文组织结构

本报告总共分为 5 个主要章节，组织结构如下：

第 1 章 引言。主要介绍跨链的背景、国内外研究现状、报告的研究目的和意义以及报告的整体结构。

第 2 章 基本概念及研究方法。主要介绍区块链基础知识、现有区块链平台、跨链目标以及跨链机制概念。

第 3 章 现有跨链技术对比分析。按跨链机制分类并在各小节分别展开讨论，介绍基于该跨链机制的典型项目、项目间的横向对比，并给出简要的总结。

第 4 章 进一步讨论。进行不同跨链机制间技术性和非技术性（性能）的对比分析，统计了研究项目中提到的技术难点，并给出了相应的解决方案。

第 5 章 总结与展望。对于跨链相关的整体工作进行总结，并对未来工作进行展望。

第2章 基本概念及研究方法

2.1 区块链概述

作为跨链技术的基础与前提，区块链技术本身拥有着诸多技术特性如稳定性、安全性、不可篡改性等。本节对区块链自身的类型、结构进行简要介绍，同时也对区块链系统中的共识机制与智能合约加以概念化说明。

2.1.1 区块链类型

区块链可依据其成员准入条件分为公有链、联盟链和私有链[17]，这种方式也是项目开发与技术选型时首要考虑的分类方式。不同类型的区块链系统将决定项目分布式账本的公开程度，与具体应用情景与业务需求紧密相关。

公有链开放程度最高，网络中任何人都可以参与至区块链系统中执行读取信息、发送交易等操作。公有链在全网开放，允许成员自由地加入或退出网络无需授权验证，数据也由大家共同记录与维护，真正地实现了去中心化交易。典型项目有比特币、以太坊等。

相对于公有链，私有链有着最严格的准入机制，只为企业内部或满足特殊条件的人群开放。其本身也是专门为私有机构或企业内部设计，交易信息不对外公布，具有节点数少、交易速度快、安全保障度更高等特点。

联盟链开放程度介于公有链与私有链之间，网络规模也处于全球与个体企业之中，更多应用于企业联盟或大型集团。联盟链中通常设有组织的概念，每个组织分管一部分节点，共同记录与维护分布式账本。交易的合法性通常需要大多数或全体组织确认才可写入区块。

2.1.2 区块链架构与模型

2016 年，袁勇等人提出了区块链基础架构的六层模型[18]，自底向上分别为数据层、网络层、共识层、激励层、合约层和应用层，详见图 2-1。

图 2-1：区块链的基础架构模型[18]

（1）数据层

区块链是由各个区块通过密码学算法顺序链接而形成的一种链式数据结构。链中各个区块依据时间顺序排序，通过记录上一区块哈希值以保证寻找到唯一父区块，形成链表结构。链中第一个区块被称为“创世区块”（Genesis Block），一般用于网络初始化，不记录交易信息。

链中其他各区块主要分为两部分：区块头（Block Header）和区块体（Block）[19]。区块头中主要记录区块元数据，用于表识区块属性以及识别每一个区块。区块头信息主要包含：1、父区块哈希：通过记录上一区块哈希实现链式结构；2、默克尔树：用于归纳并校验区块交易数据的树根信息；3、时间戳：准确记录区块生成时间；4、区块高度：区块顺序编号；5、在工作量证明中还会加入挖矿难度与随机值等信息。

区块链主体功能均包含于区块头信息中，除上述之外还有区块大小、交易总金额、交易量等属性信息。区块体则主要记录详细数据信息，包括用户私钥、交易情况、数字签名等。

（2）网络层

网络层指定了分散的通信模型以及分布式网络、数据转发和验证的相关机制。区块链通过 P2P 网络运行，节点侦听网络，并根据预定义的检查表验证广播的数据或区块。无效块将被丢弃，有效块将被转发到相邻节点，只有大多数人接受的区块才能被记入到区块链中。区块链数据存储在每个节点上，即使发生故障，也可以进行同步和恢复。区块链将具有多个中央服务器的云模型演化为完全分散的模型，有利于分散实体之间的通信和交互[20]。

（3）共识层

共识机制保证了区块链中对等节点有效合作，通过建立一套算法机制保证参与区块链中的各个节点按照预先约定的规则共同维护账本，为各节点之间建立一种信任关系。不同项目或在原有机制的基础上加以改进，或创新性地提出新的共识算法，导致目前共识机制类型繁多。但最经典、最常见的共识机制包括 PoW（Proof of Work，工作量证明机制）、PoS（Proof of Stake，权益证明机制）、DPoS（Delegated Proof of Stake，授权股权证明机制）、PBFT（Practical Byzantine Fault Tolerance，实用拜占庭容错算法）等[21]。

PoW 通过对需要大量计算的数学任务求解以获得记账权和奖励，通常体现在挖矿机器算力的高低，实现了完全去中心化；PoS 依据持有币数量和持有时间发放利息，相比 PoW 更节能，共识达成时间更快；DPoS 中持币人可以投票选举代理人，记账与验证均由代理人执行。这种方式缩小参与节点数量，可实现秒级验证；PBFT 中允许链上所有人投票，结果依据拜占庭容错算法处理。换言之就是以“少数服从多数”选举领导并进行记账共识。

（4）激励层

激励层将经济激励整合到区块链技术体系中，主要包括经济激励的发行机制和分配机制。例如，每创建新的区块，就会发行一定数量的加密货币作为奖励，并将其分配给获胜的节点，以激励整个网络继续进行数据验证和区块创建。激励层能够为区块链提供驱动力，也可以在区块链中建立基于加密货币的金融系统，以便可以轻松支持非中介交易和实时小额支付。激励层对于某些部分集中的区块链应用程序是可选的，多中心化的联盟链和完全中心化的私有链可能并不需要设计激励层中的经济激励，即“无币区块链”[18]。

（5）合约层

智能合约为区块链提供可以自动运行的协议条款。其本质是一段计算机程序，通过高级程序设计语言如 Java、Golang 等进行编写。智能合约可以由区块链激活、启动并运行，并严格按照预先约定的规则执行交易[22]。

智能合约的出现取代了人为合约仲裁，以计算机自动化方式执行协议条款这种方式有效地提高了合约执行效率和成本。同时合约是对外公开的，运行在区块链系统提供的容器中，保证了交易公平透明和结果真实唯一。区块链中智能合约一旦部署则永久运行于各个对等节点中，如同法律认可的纸质条款，保证每时每刻均有效力。

（6）应用层

应用层封装了区块链的各种应用场景和案例。区块链不仅仅可用于加密货币领域，还可用于经济、金融和社会系统中。

2.2 主流区块链底层技术平台

随着跨链技术逐渐发展，各大区块链网络也提出或引入了跨链通信解决方案。本节对现有的主流区块链平台及其跨链相关内容进行简要介绍。

2.2.1 Bitcoin

比特币是当下分布范围最广、交易市值最大的区块公有链[1]。通过 PoW 共识机制，牺牲效率保证了交易的安全性与可信度，是首个实现去中心化货币交易的项目。比特币的发行与流通均通过网络开源的点对点算法实现，没有发行机构控制，也不受国境约束。

作为区块链技术的起源项目，围绕比特币衍生出诸多区块链技术，其中不乏区块链跨链技术。RootStock、闪电网络都是基于比特币开发的跨链项目，也有区块链通过侧链锚定方式与比特币互通，实现跨链需求。

2.2.2 Ethereum

以太坊[23]作为第二代区块链技术代表，是全球开源的分布式应用开发平台。以太坊旨在解决比特币缺乏图灵完备脚本开发语言的弊端，开发者可以通过智能合约开发分布式应用程序，用于在各个应用领域实现普及。

在区块链互操作性解决方案上，以太坊的 BTC Relay 也首先提出了侧链机制并实现了和比特币的互通，随后完善并发展为跨链主流方案之一：侧链/中继技术。Wanchain 也基于以太坊实现跨链通信协议，完成链间互通。

2.2.3 EOS

EOS[2]被视为区块链 3.0 技术的典型，其定位与以太坊相似，希望实现去中心化应用平台和区块链底层基础设施。EOS 全称 Enterprise Operation System，被认为是一种企业级区块链操作系统，能够满足各行业真实业务场景需要。其共识机制融合 dPoS 与 BFT，一定程度上解决 PoS 的缺陷，具有较高的交易执行

效率和低廉的交易成本。EOS 在设计之初就考虑到互操作性，支持跨链交付，包括与子链、侧链的数据互通。后续开发中也考虑通过引入跨链协议实现与比特币和以太坊的跨链互通。

2.2.4 Hyperledger 系列

Hyperledger 旨在推动区块链的跨行业应用，创建开放的、跨国界、跨产业的区块链技术标准[24]。Hyperledger 旗下有诸多子项目，包括 Fabric、Sawtooth、Quilt 等近十项。其中 Fabric 最为核心，提供了一个模块化的具有权限控制系统的联盟链底层开发框架。项目 Sawtooth 使用时间流逝证明（Proof of Elapsed Time）机制，也支持多语言编写智能合约。跨链方面 Hyperledger Quilt 通过 Java 实现了 Interledger 跨链协议 ILP，为账本系统之间提供互操作性。Quilt 也因而成为 Hyperledger 项目的跨链解决方案，用于连接不同区块链系统。

2.2.5 Multichain

Multichain[25]是一个即用型私有链搭建平台，可以通过简单的部署与配置快速完成私有区块链的构建与运行。Multichain 采用 PoA 共识机制，通过权限治理方案保证私有链的隐私与保密性。在互操作性上，Multichain 实现了对比特币的向后兼容，实现私有链与公有链信息传递与资产转移。Multichain 也可以通过配置实现对不同区块链的同时支持，完成私有链和比特币区块链的价值转换。

2.2.6 比较

目前区块链平台尚未出现真正的统一，各大平台项目均有技术特性与发展空间，在未来的地位与重要性不可预知。本节对上述五个相对主流的区块链平台进行简要对比与分析，类型依照其准入机制划分为公有链、联盟链与私有链；出块时间指生成一个区块的平均时间。

表 2-1 区块链平台技术对比

项目名称	类型	共识机制	出块时间/秒
Bitcoin	公有链	PoW	600
Ethereum	公有链	PoW	15
EOS	公有链	dPoS+BFT	0.5
Hyperledger	联盟链	PoET	默认 20
Multichain	私有链	PoA	默认 15

对于公有链项目，也可以通过区块链浏览器对比其实时运行数据与交易行情分析项目本身的运行使用情况，对比见表 2-2。

表 2-2 区块链平台交易行情对比

项目名称	区块高度	交易总数	持币地址数	流通总量	价值
Bitcoin	641,896	554,548,215	31,241,293	18,449,127	$11,172.00
Ethereum	10,580,975	785,576,347	44,986,085	109,303,744	$370.63
EOS	134,471,719	4,492,051,220	2,006,077	934,850,023	$2.97

注：（调研时间为 2020 年 8 月 2 日 22:45:38）

根据表 2-2 中数据可知，EOS 发展态势良好，由于其较成熟的共识机制算法与快速的出块时间，使其区块高度与交易总数均占优势，货币流通总量大。

但是尽管如此，比特币和以太坊依旧在区块链平台领域有着相当的地位，有着庞大的持币地址数及高额的货币价值，作为目前最主流区块链系统提供交易服务。

2.3 区块链跨链技术

跨链技术是一种新兴技术，可增强区块链之间的互操作性，从而实现各种网络之间的价值和信息交换。跨链为区块链大规模采用奠定了基础，有潜力解决一直困扰着区块链生态系统的可扩展性问题。

2.3.1 概念

跨链技术尚且未有业界公认的定义。结合跨链的目标，本文认为跨链技术能够实现区块链之间的互操作，以解决现有去中心化技术之间缺乏沟通的问题，打破分散的孤岛。典型的跨链目标包括跨链交换、跨链资产转移、跨链 Oracle、跨链资产留置、跨链智能合约五类[26]。

1） **跨链交换：**跨链交换允许双方交换来自不同区块链的资产（Token）。双方都需要在每个区块链上有一个账户或地址。跨链交换中每个链上的资产总量不变，资产所有权改变。交易在两个区块链上同时执行，即所有权变更同时发生。

2） **跨链资产转移：**资产转移允许用户将资产从一个区块链转移到另一个区块链，将原链上的资产进行锁定，在另一个链上重新铸造等量等值的资产。这个连接应该是双向的，也允许在任何时刻将资产转移回来。各个链上的资产总量随着转移的发生产生相应的增减。

3） **跨链 Oracle：**Oracle 为区块链提供外部数据，即数据来自另一个区块链。例如，Oracle 从区块链 A 中提取有关交易的信息，然后触发区块链 B 上的一个事件。

4） **跨链资产留置：**跨链资产留置能够在一个区块链上锁定资产并在满足另一个链上的特定条件时将其解锁。 类似于金融中的产权抵押或保证金。

5） **跨链智能合约：**跨链智能合约实现区块链之间的无缝依赖，在多个链中有多个依赖。例如，跨链智能合约可以通过检查用户在区块链 A 上的股权证明在区块链 B 上用 B 的货币发放股息。跨链智能合约也能实现其他的一些用例。

2.3.2 基本原理

w a n g

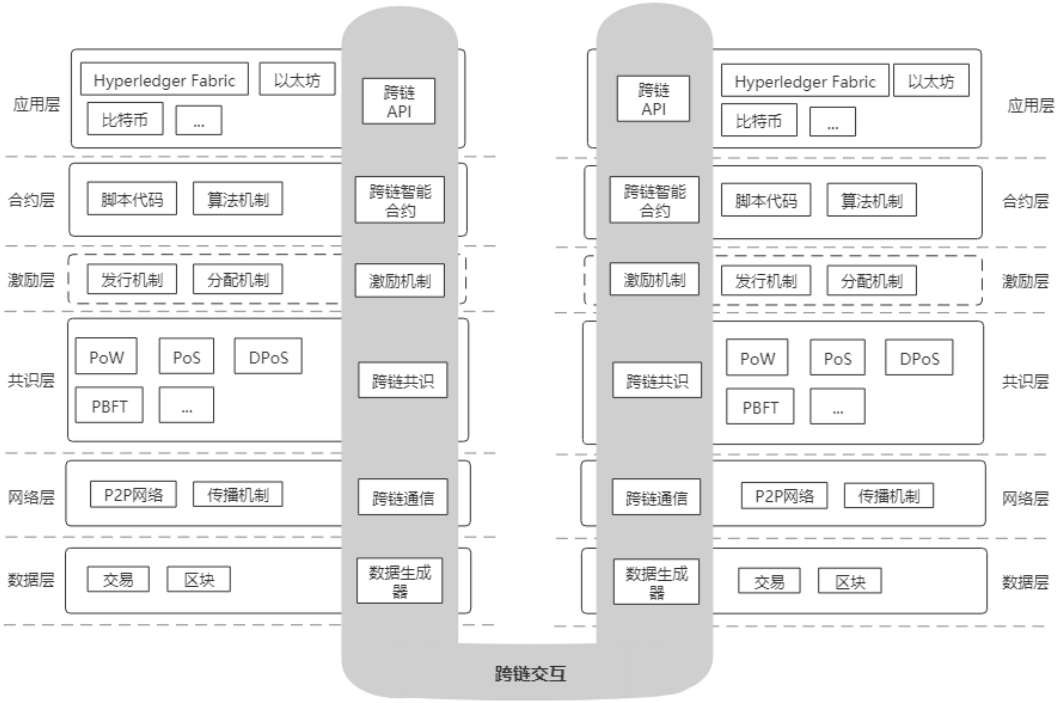

图 2-2：跨链层级架构图

在本节中，参考 Hai Jin 等人的跨链总体架构图并将其普适化[7]，我们展示了一个基于区块链六层模型的跨链框架，见图 2-2。接下来，我们将详细介绍每层中模块的设计及挑战。

（1）数据层

不同的区块链系统在数据层方面会有所不同。交易格式的多样性是阻碍不同链交互的挑战之一。例如，以太坊和比特币的交易格式不同，这会阻碍它们进行交易的直接传播。可以采用统一交易格式，但改变现有区块链系统的交易格式会增加复杂性，也可以使用交易翻译器将交易从特定格式转换为通用格式。

（2）网络层

许多区块链的网络层设计仅考虑了内部通信，需要扩展到跨链通信。跨链通信可能会遇到的问题包括：1.没有中央服务器或授权机构来获取对方区块链

中节点的 IP 地址。2.如何实现跨链通信的良好性能，通信可分为主动（例如轮询）和被动（例如等待）模式，存在效率低下的问题。

（3）共识层

共识协议的功能是维持区块链系统状态的正确性，在跨链交互上下文中，共识层可用于验证，验证协议将验证数据是否已在源链中提交，以及传输的数据是否被篡改。

（4）激励层

由于激励层是可选的，有些区块链并不需要经济激励。在跨链的情况下，一些场景也无需激励。部分跨链实现中包含了验证者（validator），验证者的行为可能会使用激励机制来管理或约束。

（5）合约层

将智能合约扩展到跨链场景，合约应该分别由来自两个链的两个条件触发。跨链智能合约的挑战之一是如何统一合约运行时的环境和编程语言，因为各区块链系统可能采用不同的执行时间和语言。

（6）应用层

我们需要释放跨链应用程序更多的可能性。应用层在跨链场景下一个简单的挑战是，大多数跨链通信都是从界面中抽象出来的，该如何提供友好的开发界面。

我们在后文中对不同的项目进行支持平台、验证机制、通讯（通信）协议、共识机制、应用场景以及优缺点方面的横向比较。其中支持平台和应用场景与应用层有关；部分应用场景中包括跨链智能合约，它与合约层有关；共识协议位于共识层；通信协议与网络层相关；部分通信协议通过抽象区块结构、统一跨链消息格式来实现，涉及到了数据层；部分验证机制中验证者的管理与激励层有关，网络传输过程会使用验证机制确保数据的准确性，验证机制也与共识层相关。

2.3.3 跨链机制

区块链跨链技术方案依据其具体实现方法可以分为五类：公证人机制、侧链/中继、分布式私钥控制、哈希锁定和区块链分片，本节将对此进行基础概念的介绍。

1. 公证人机制

公证人机制使用受信任的个人或团体作为公证人，来向区块链 X 声明区块链 Y 上发生了某些事情，确保提供的信息正确无误[7]。公证人机制是双向跨链，可以实现跨链资产交换及转移，利用智能合约在链与链间操作。

公证人机制和其他跨链机制相比较为简单，基础区块链不需要任何更改，但是公证人需要信任。为了实现公证人的可信，其中一个解决方案是，X 和 Y 两个区块链都可以选择他们信任的一组公证人，然后可以使用共识算法（例如 BFT）创建公证人输出，这种情况下，并不要求信任所有公证人，只需信任一组公证人的三分之二即可。公证人组既可以自动侦听和响应事件，也可以在请求时侦听和响应事件。

公证人机制可分为中心化/单签名公证人机制，多重签名公证人机制和分布式签名公证人机制。

（1） 中心化/单签名公证人机制（Centralized Notary schemes）

公证人通常由单一指定的独立节点或者机构充当，它同时承担了数据收集、交易确认、交易验证的任务。这是最简单的模式，但是中心节点安全性是系统稳定的关键瓶颈。

（2） 多重签名[1]公证人机制（ Multi-sig Notary schemes）

多重签名公证人的每一个节点都拥有自己的一个密钥，只有当达到一定数量或比例的公证人在各自账本上共同签名达成共识后，跨链交易才能被确认。多重签名的安全性更高，但是两条互操作的区块链本身需要支持多重签名。

（3） 分布式签名公证人机制（Distributed Signature Notary schemes）

与多重签名公证人机制的签名方式不同，它采用了多方计算[2]（MPC, Multi-Party Computation）的思想，安全性更高，实现也更复杂。

2. 侧链/中继机制

侧链是连接到中央分布式分类帐（主链）的从属分布式分类帐[8]。它在技术上独立于主链，可以拥有自己的共识机制、通证（Token）和用户。侧链能够拥有主链的功能，可以读取和验证主链中的数据，并且可以在主链的基础上添加交易隐私保护技术、智能合约等新功能。

中继可看作是侧链技术的一种特殊形式，中继是链与链之间的通道，通过中继可以将一个区块链的信息提供给另一区块链，如果通道本身是区块链，那

[1] 多重签名意味着在交易发生之前需要多方签名或批准。多重签名会增加加密货币的安全性，这样一个人就不能在未经他人同意的情况下把所有的数字货币都拿走，使签署方可以验证多重签名交易并对其负责。

[2] 多方计算是一种技术事件，在这种技术中，多个互不信任的计算机可以在较大数据集的各自唯一片段上进行计算，从而共同产生所需的公共事务。

就是中继链。中继提供了以分散方式验证跨区块链交易的能力，代替了可信的中介机构，更加灵活且易于扩展。

侧链通常使用简单支付验证（SPV，Simplified Payment Verification）来验证交易已经在区块链中发生，SPV 证明包括一组区块头的列表（包含 Merkle Root）和一个特定输出（output）存在于某个区块中的密码学证明。

最初，仅允许从主链到侧链一个方向上进行资产转移或转发信息，称为单向锚定（one-way peg）。后来，Greg Maxwell 提出了双向锚定（two-way peg），即价值可以转移到另一个链上，然后再回到原先的链上。双向锚定的协议改造需兼容现有主链，具体实现方式有：单一托管模式、联盟模式、SPV 模式、驱动链模式、混合模式。

侧链/中继机制能支持跨链资产交换和转移、跨链合约和资产留置。侧链增强了可扩展性，既利用了主链网络特性，提高了交易速度，又不会给主链造成负担。

3. 分布式私钥控制机制

分布式私钥控制技术通过分布式节点控制私钥，将源链加密资产映射到基于区块链协议的目标链上，并根据交易信息部署新的智能合约、创建新的加密资产[8]。在代币转入目标链后，跨链操作节点会基于智能合约进行代币发放，从而实现资产跨链转移。

分布式技术关键在于对源链上代币管理权的控制，通过 Lock-in（锁定）和 Lock-out（解锁）两种互逆操作实现。锁定时将密钥分片并保存到多个分布式节点中，实现分布式控制权管理和资产映射。解锁时通过对分布式保存的私钥进行验证，使代币由原来的锁定状态转换为可操作状态。跨链后原有财产的私钥由去中心化网络保存，用户拥有映射后的跨链代理资产私钥；解锁时用户释放映射资产私钥，获取原有资产私钥，即获得原有资产控制权。

这种方式下，私钥只由用户和去中心化网络共同掌管，不存在第三方参与。此外用户掌握部分私钥，并没有失去对财产的控制权，安全性更高。

4. 哈希锁定机制

哈希锁定技术是一种要求交易方在限定时间内对哈希值原值进行猜测以完成支付的机制，依赖于哈希函数的单向性与低碰撞性。哈希锁定技术起源于闪电网络，最初用于支持快速小额支付，后来用于到跨链技术中。哈希锁定中交易需要满足两个条件：1、哈希锁，只有提供目标哈希的原像才能完成交易。2、时间锁，需要在限定时间内完成。哈希锁定技术实现了无需信任的链间交易，提高交易速度的同时有着较好的安全性[8]。

原子互换技术（Atomic Swaps）又称原子转移（atomic transfer），使用了哈希时间锁定协议（HTLAs），其本身是在不同类型资产间提高无需信任的点对点交易服务，保证交易动作的完全执行或完全不执行。这种技术去中心化的优势很好地传承至哈希锁定技术，消除第三方中介，减少交易时间与交易成本。

哈希锁定技术仍有不少缺陷，哈希锁定的时间锁严格依赖时间差，对于时间要求高的交易难以契合需求。在时间设定上也很有可能出现人工失误，不够智能化。此外，对于交易本身，哈希锁定只能做到交换，无法实现更复杂的资产转移或信息传递，使用场景受限。哈希锁定的一系列技术挑战决定其无法成为跨链主流技术，仍存在较大改进空间。

5. 区块链分片机制

分片是一种将计算和存储工作负载分散到对等网络上的分区方法，这样每个节点就不必负责处理整个网络的事务负载。当分片应用于区块链时，每个节点只拥有和维护区块链上的一部分（与其分区或分片相关的）数据。节点以共享的方式维护分片上的信息，在分片中仍然保持分散。同时，每个节点并不加载整个区块链上的信息，因此有助于提高可伸缩性和事务吞吐量，解决延迟问题，降低交易成本[27]。

POW 共识算法不能与分片结合使用，因为一个节点无法在只有一个（其所属）分片信息的情况下参与事务验证。通常使用 PoS 共识算法，标识每个分片中负责事务验证的权益人（stakers）。

虽然在一个分片内的节点之间的通信是平稳的，但是分片之间的通信目前并不容易，需要开发一个单独的协议。除此以外，权力下放和透明度使得维护安全变得困难，单一碎片攻击等问题也是面临的难点。

2.4 本章小结

在深入探索或者实践区块链跨链之前，我们需要了解一些基础知识和概念。本章主要分为两部分，一部分有关区块链，介绍了区块链的类型、结构、共识机制和智能合约以及现有的区块链平台；另一部分有关跨链，介绍了跨链的目标（应用场景）以及多种跨链机制。这些基础概念将为下文进一步调研提供理论依据。

第3章 现有跨链技术对比分析

本文调研了共 103 个跨链项目，所实现的跨链机制包括上一章节所述的侧链/中继链机制（41.75%）、公证人机制（9.71%）、哈希锁定机制（5.83%）、分片机制（4.85%）和分布式私钥控制机制（2.91%）。可以发现，侧链/中继链机制是目前在跨链项目中应用最为普遍的，热门项目 Polkadot 和 Cosmos 均采用了该机制。除此之外，有 34.95%的项目并没有明确提及跨链机制或是使用了其他技术来实现跨链，例如通过定义通信协议（通信协议簇）等。

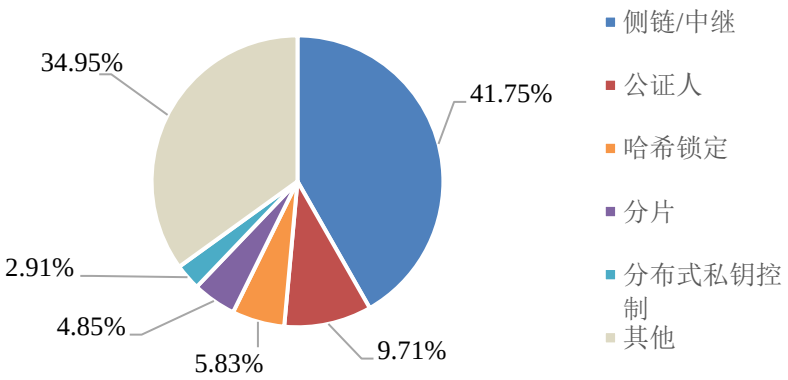

图 3-1：现有跨链技术解决方案所依据的跨链机制分类情况

本文所检索到的 103 个跨链技术解决方案的发布时间分布见图 3-2。最早的跨链项目开始于 2014 年，在 2014 年到 2018 年间，跨链项目数量逐年增长。2019 年和 2020 年项目数量减少一是因为部分项目较新，至今尚未成熟地开发和发布；二是因为项目提出时间较短，信息量较少，我们的项目列表中并未统计到它们。

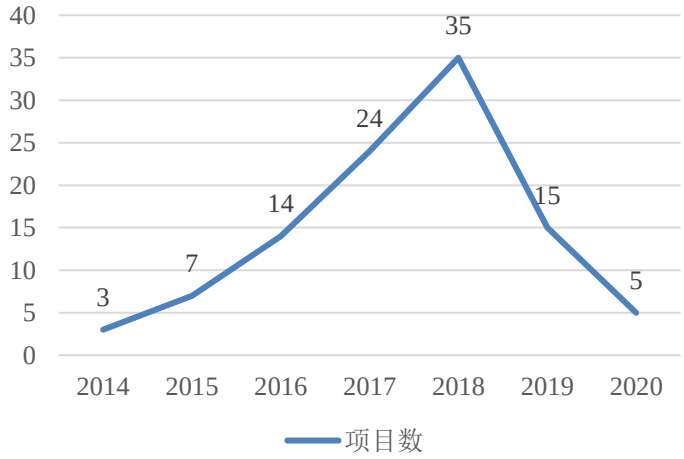

图 3-2：项目发布时间分布图

本文综合对比 103 个项目的 Github 数据（浏览数、收藏数、克隆数）、谷歌搜索返回结果数、百度搜索返回结果数，最终共筛选出 22 个典型项目。本文进一步统计了所选的典型跨链项目两侧支持的区块链平台类型，统计结果如下图 3-3 所示。从图中可以看出，被比特币（45.45%）、以太坊（36.36%）和 Hyperledger Fabric（13.63%）这三种类型的支持比重最高，除此之外，还包括 EOS、FISCO BCOS 等。从另一个维度来看，以 EKT 为代表的跨链项目仅支持公链间的互操作；而 BitXHub 等目前仅支持联盟链间的互操作；相比较而言，Ripple、Kepler 等项目则支持多种类型（私链、公链、联盟链）的区块链之间的互操作。

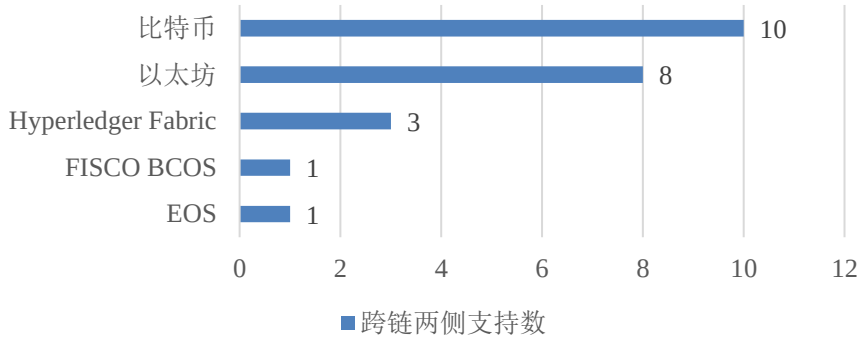

图 3-3：跨链两侧支持的区块链

本文进而对每一类跨链机制下的典型项目进行详细分析和横向对比，来帮助回答第一章所设定的研究问题 2，即所探究的跨链技术方案如何应对区块链的互操作性需求。

3.1 侧链/中继机制

3.1.1 总体概述

侧链/中继技术解决方案架构一般如图 3-4 所示。各个项目的具体设计与应用环境各不相同，因而项目间具体架构也存在较大差异。但其主主体结构均为通过跨链协议，以中继链或其他中介方式沟通各个异构区块链网络，实现多链互通。

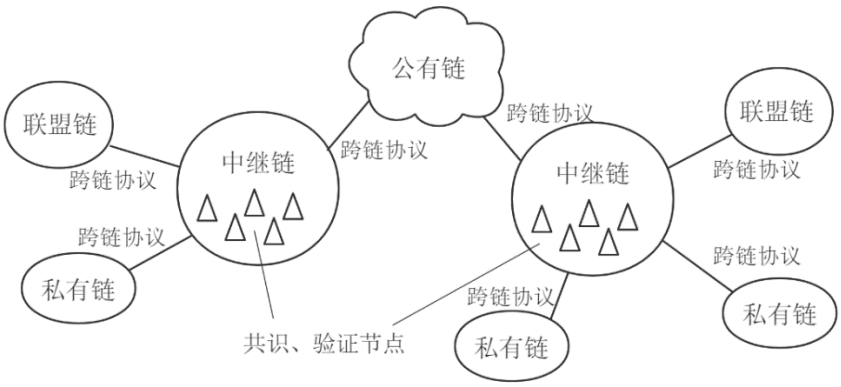

图 3-4：侧链/中继的跨链解决方案图

3.1.2 基于侧链/中继机制的典型跨链解决方案

1. 方案实例介绍

（1） BTC Relay

BTC Relay[28]是由区块链软件技术公司 ConsenSys 基于以太坊实现的跨链智能合约，被认为是比特币的第一个侧链。以太坊能够验证比特币网络上的交易，提高了以太坊的可扩展性，是跨链资产转移的一次有意义的尝试。

BTC Relay 不断接受网络中各 Relayer 节点推送的比特币交易数据，即区块头 hash 数据，在检验其有效性正确之后，以链表的方式存储并维护。交易数据主要以 Merkle 树的形式存储，因此只需提交交易信息和 merkle 路径即可验证交易合法性。

BTC Relay 以一种去中心化的方式实现了比特币与以太坊之间的跨链资产流动，其简单的原理使得 BTC Relay 易于实现于应用。但 BTC Relay 只能处理比特币与以太坊之间互通，缺乏通用性；是一次有效的尝试，但缺乏改进。

（2） Cosmos

Cosmos[29]是一个由独立的平行区块链组成的分布式网络，各个链上均由 BFT 算法支持。Cosmos 构建了一种区块链生态系统，关键特性在于其优秀的互操作性和可扩展性。

Cosmos 架构由枢纽（Hub）和分区（Zone）构成，枢纽是用于处理跨链事务的中继链，分区是 Cosmos 平行链，可以用于外部区块链的接入。Cosmos 设计了跨链交互协议 IBC（Inter-Blockchain Communication Protocol）用于支持分区间互操作，而无需分区具有交换流动性（Exchange liquidity）；同时结合基于拜占庭容错算法提出 Tendermint 共识机制实现分区扩展与跨链价值流动。

传统项目将整个网络作为一个整体管理，而 Cosmos 每个应用都有自己的网络、共识层与治理方式，开发者拥有很大的自主性，因而 Cosmos 不会被意识分歧所束缚，具有更好的扩展性，能够支持更大规模的网络体系。

BSN 开发团队正在建立 BSN 的跨链通讯枢纽（Interchain Communications Hub，ICH）[15]。IRISnet 是支持分布式应用程序的链间服务枢纽，IRITA（Inter-Realm Industry Trust Alliance）是其联盟链产品。IRITA 作为 Cosmos 生态下首个企业级联盟链产品，有着与 Cosmos 类似的技术框架、通讯协议和共识机制，可支持异构链间通信。通过使用 IRITA 的链间服务枢纽，Chainlink 将被集成到 BSN 网络中。集成 Chainlink 预言机后的 BSN 跨链通讯枢纽可让 DApp 获取 BSN 之外的可信数据。

（3） Polkadot

Polkadot[30]可以实现无信任数据传输、消息传递、价值流动的平台，是一种可扩展的异构多链技术。Polkadot 最显著的特性包括：共享安全性和无信任跨链交易。作为新一代区块链协议，Polkadot 能够整合各个网络协同工作，解锁诸多应用场景。

Polkadot 网络包括 4 种角色：收集者（Collator）、渔夫（Fisherman）、提名者（Nominator）和验证者（Validator），分别用于收集交易与生成证明、监控恶意行为、拥有权益并委托资产、验证交易并添加区块。链间互操作性上基于其跨链协议 XCMP（Cross-chain Message Passing，跨链消息传递），Polkadot 能够通过中继链在各个平行链之间发送消息且无需信任。通过设计参与方角色、激励模型，Polkadot 成为可自发扩展、兼容已有区块链的异构多链网络。

（4） RootStock（RSK）

Rootstock[31]是比特币的双向锚定侧链，旨在为比特币生态系统提供图灵完备的智能合约功能。由于比特币无法验证另一个区块链上余额的真实性，故发生转移时，某些 BTC 会锁定在比特币中，而相同数量的 SmartBitcoin（SBTC）会在 RSK 中解锁，SBTC 转换回 BTC 时同理。

由于比特币目前不支持智能合约或本机操作码来验证外部 SPV 证明，因此 RSK 中双向锚定的一部分需要对半信任的第三方（Semi-Ttrusted Third-Parties，STTP）的信任。STTP 临时存储已锁定的 BTC，并解锁 BTC 以从 RSK 中的 SBTC转回比特币。资金的锁定和解锁是通过安全的网络节点完成的，无需人工干预。

RSK 网络通过联合挖掘和联盟检查点机制得到保护，有效地允许它保留比特币的双花证明和结算最终性的安全性。

（5） BitXHub

BitXHub[32]由中继链、应用链和跨链网关组成。中继链用于应用链管理、跨链交易可信验证和可靠路由，并实现了 跨链传输协议（Inter-Blockchain Transfer Protocol，IBTP）。跨链网关用于在区块链之间收集和传播交易，它不仅支持应用链和中继链，还支持中继链和中继链之间的交互。应用链分为同构链和异构链，负责具体的业务逻辑。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，相同的共识算法和加密机制等；异构应用链不直接支持 IBTP 协议，如 Hyperledger Fabric、以太坊等。

BitXHub 的核心功能特性包括：a）通用的跨链传输协议 IBTP，支持异构区块链之间的跨链交易路由和可信验证，允许异构资产、数据及服务的跨链调用；b）异构交易验证，中继链提供可插拔的跨链验证引擎，支持异构应用链的交易验证规则的动态注入，并通过并行跨链验证技术提供高效的代理验证服务；c）多层级路由，通过跨链域名管理机制实现异构层级链之间的交易高效路由，基于哈希锁定的信任传递机制实现异构层级链之间的可信价值传递。

2. 方案横向对比

基于侧链/中继机制的跨链项目所支持的平台、跨链类型、消息验证机制及技术类型对比见表 3-1。基于 BTC 区块链是指该项目在比特币（BTC）基础上提出或开发（例如 Pegged Sidechains）、或属于比特币的侧链（例如 Rootstock）、或是比特币特性的一部分；基于 ETH（以太坊）区块链类似；自有链的跨链技术基于或属于非比特币/以太坊的其他区块链，主要致力于实现通用、标准化的区块链接入模型。在之后的小节中，我们也对不同项目就此项进行陈列，之后将不再重复说明。

表 3-1 基于侧链/中继的项目间平台、跨链类型、消息验证、侧链/中继对比

项目名称	平台	跨链类型	消息验证机制	侧链/中继
BTC Relay	基于 ETH 区块链	异构（BTC，ETH 等）	SPV	侧链（单向锚定）
Cosmos	自有链	异构（以太坊、Zerocash、比特币、CryptoNote、IRISnet、IRITA 、Kava、Paradigm 等，满足 zone 要求的区块链）	SPV	中继（双向锚定）
Polkadot	自有链	异构（基于其平行链模型设计的区块链）	多个验证者进行验证	中继（双向锚定）

RootStock（RSK）	基于 BTC 区块链	同构（比特币、RSK）	联盟（半信任第三方）	侧链（双向锚定）
BitXHub	自有链	异构（Hyperledger Fabric、趣链区块链平台）	可插拔的跨链验证引擎	中继（双向锚定）

根据对比可以看到，BTC Relay 作为首个跨链项目采用单向锚定，在技术发展后其他项目均采用双向锚定实现跨链互通。BTC Relay 和 Cosmos 使用 SPV 进行验证；Polkadot 通过多个验证节点判断事务；RootStock 依赖于被称为联盟的半信任第三方，此外联盟还将帮助减轻联合挖矿（Merged Mining）的危险；BitXHub 通过跨链验证引擎支持交易验证规则动态注入，其并行跨链验证技术可提供高效代理验证服务。相比于其它项目，RootStock 关注于对比特币功能的扩展，跨链应用也主要作为侧链与比特币互通，因而归属于同构跨链。

通讯协议列表见表 3-2，各个项目都有自己的通讯协议支持。但其中特殊的是 BTC Relay 并没有明确的协议规范，而是通过 Relayers 节点发送区块头的方式实现跨链交易。

表 3-2 基于侧链/中继的项目间通讯协议对比

项目名称	通讯协议	简介
BTC Relay	区块头中继（block header relaying）	比特币区块头（block header）信息存入 Relayers 智能合约中，实现以太坊上基于 SPV 验证交易有效性
Cosmos	IBC	Cosmos 枢纽与分区间通信协议，基于区块虚拟的 UDP 或 TCP 协议，保证跨链资产转移的安全高效
Polkadot	XCMP	统一寻址协议，通过基于 Merkle 树的简单队列机制解决跨链事务，保证交易准确有效
RootStock（RSK）	2SBP，PMT，DTI，IBHP，2PSC，LRO	双存储区块传输（2SBP），推送丢失传输协议（PMT），延迟传输交易包探试（DTI），区块头先行传播（IBHP），双优先流连接协议（2PSC），本地路由优化协议（LRO）
BitXHub	IBTP	抽象区块结构，统一跨链消息格式，确定路由寻址

BTC Relay 使用经典的工作量证明机制，其余项目均在共识机制上加以改进。基于 GHOST 的递归祖先派生前缀协议（GHOST-based Recursive ANcestor Deriving Prefix Agreement，GRANDPA）在 Polkadot 中继链上运行，允许验证者对某个有效的、高度最高的区块进行投票，该方法可以快速验证区块，容纳大

量验证节点；Cosmos 要求共识算法满足区块链应用接口（Application BlockChain Interface，ABCI）规范以保证通信标准化，唯一符合的 Tendermint 则通过每个验证者的信息交流判断某个区块的取舍，能够实现异地同步；RootStock 的“混合”安全模式同时包含了 PoW 机制和私人网络模式，基于联合的门限签名方案实现安全联合工作量证明挖矿机制，使用一种名为“DECOR +”的区块奖励分享方案来减少竞争，并允许矿工延迟切换到 Rootstock 最佳区块。BitXHub 可插拔特性用以方便接入不同种类的共识算法。

D 表 3-3 基于侧链/中继的项目间共识机制对比

项目名称	共识机制
BTC Relay	PoW
Cosmos	Tendermint（基于 PBFT）
Polkadot	GRANDPA
RootStock（RSK）	安全联合工作量证明，DECOR +
BitXHub	可插拔共识算法插件

表 3-4 中列出了各个项目适用的应用环境。

表 3-4 基于侧链/中继的项目间应用场景对比

项目名称	应用场景
BTC Relay	验证比特币事务；跨链资产交换
Cosmos	分布式交易所；跨链交易；多应用集成；网络分区缓解；
Polkadot	资产跨链、分布式应用开发、生态领域开发：数字身份、社交平台等
RootStock（RSK）	资产转移，Rootstock 使用比特币作为一种燃料运行 Rootstock 智能合约
BitXHub	跨链交易的捕获、传输以及验证，资产互换，数据互通及服务互补

如表 3-4 所示，相比于其他机制，Cosmos 和 Polkadot 注重于区块链生态系统的搭建而不再关注与某一具体领域，意图在于作为一种基础设施提供各种场景下的服务。BitXHub 更专注于异构和同构联盟链间的互操作，实现跨链服务。

上述各项目特性归纳见表 3-5。

表 3-5 基于侧链/中继的项目间特性对比

项目名称	特性
BTC Relay	1、区块链生态系统公认的第一条侧链，首次实现了比特币跨链资产流动
Cosmos	1、设计共识引擎 Tendermint，兼具高适应性、高性能、高安全性等特点 2、架构简单有效，较好地平衡区块链的可扩展性、安全性及性能 3、枢纽分区架构与 IBC 通信协议结合，互操作性和可扩展性较好
Polkadot	1、互操作性：实现应用与智能合约的无缝跨链资产交易 2、可扩展性：提供多链并行的能力，理论上具有无限的扩展性 3、共享安全： Polkadot 平行链都将由中继链统一维护共识与记账
RootStock（RSK）	1、独立 VM，但在操作码级别上与 EVM 兼容 2、为以太坊用户提供了在比特币网络的安全下运行其项目的可能性 3、新的操作码用于快速的 int32 算术和更好的即时编译（计划中），以获得更好的性能
BitXHub	1、跨链传输协议 2、异构交易验证引擎 3、多层级路由

各个项目中也存在一定的限制因素。

表 3-6 基于侧链/中继的项目间限制对比

项目名称	限制
BTC Relay	1、仅支持比特币和以太坊间的跨链，且为单向通信，应用有局限性 2、Relayers 智能合约中不断存储区块头，导致其规模持续膨胀 3、Relayers 奖励机制会导致维护成本较高，而 relayers 活跃度依旧较低
Cosmos	1、每个链都需要导入自己的验证者、经济体系等成分，不可与其他链共用 2、Tendermint 算法在验证时间上有着较高的通信成本 3、Cosmos 极度依赖中心 hub，跨链有中心化趋势
Polkadot	共享安全使中继链不断安插验证节点以供二次验证，大幅增加中继链压力
RootStock（RSK）	1、合并挖矿仅提供针对外部哈希率的安全性，一般情况下无 2、无法实现不信任的双向资金桥梁（即在不信任第三方的情况下，将代币/代币从主链和侧链转移到主链和侧链）
BitXHub	1、每个中继链最多支持 64 个应用链 2、目前还未开发完，只支持单中继链跨链方式

3.1.3 总结

基于侧链/中继链实现跨链的项目有的基于比特币，有的基于以太坊，有的项目还支持异构链间的交互。除了BTC Relay，其他的侧链几乎都实现了双向锚定。这些项目常使用 SPV 进行消息验证，也有一些项目使用验证者（Validator）、半信任第三方等。通信协议通过抽象区块结构或抽象跨链消息格式实现。项目的应用场景广泛，大部分兼具高适应性、高性能和高安全性，但单向通信的项目存在局限性，且中继链结构复杂，压力较大。

3.2 公证人机制

3.2.1 总体概述

本文参考了 Jiang Y 等人[33]的绘图，抽象出基于公证人机制的跨链解决方案图，见图 3-5。公证人机制是由单个或一组节点作为一个相对独立的角色，验证来自双方的交易，只有经过公证人节点验证的交易才会传输到目的区块链。

本节中介绍了四个基于公证人机制的跨链项目：Corda、Ripple、Kepler 和 Binance（币安）。

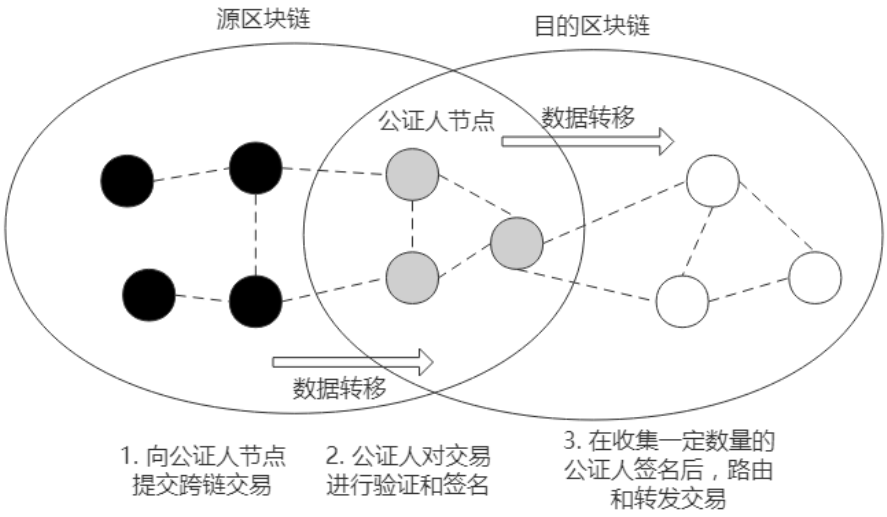

图 3-5：公证人机制的跨链解决方案图

3.2.2 基于公证人机制的典型跨链解决方案

1. 方案实例介绍

（1） Corda

Corda[34]是一个开源区块链项目，多用于记录、管理及自动化执行金融合约。

Corda网络是一个点对点网络，拥有一个或多个提供交易排序和时间戳服务的公证服务，从而将矿工在其他系统中扮演的角色抽象为一个可插拔的组件。它使用流框架（Flow Framework）管理参与者之间的通信和协商，并使用公证人来验证唯一性和有效性。公证人是一种服务，它保证只有在所有输入状态都未被使用时，它才会签署交易。一个单一的 Corda 网络可能包含多个公证人，他们使用各种不同的算法提供担保。因此 Corda 不依赖于任何特定的共识算法。

Corda中的交易不需要全网广播，只在交易关联方和验证节点之间传递，共识机制也只存于验证交易的节点之间，提高了交易性能和隐私。Corda 是基于Kotlin开发的，智能合约可以用 Java 和其他 JVM 语言编写。此外，Corda 还支持开发和部署被称为CorDapps的分布式应用程序。

（2） Ripple（Interledger）

2015年11月，Ripple公司发布了Interledger白皮书[35]，并提出了一种用于不同支付网络或账本系统间的支付协议——跨账本协议（Interledger Protocol，ILP）。有了 ILP，货币等价值可以通过支付网络和账本打包、按路线发送和交付。它承诺降低处理跨境交易所需的成本和时间。Ripple 实验室利用它在其产品中连接跨国银行系统。

Interledger 提供了一种名为连接者（Connector）的顶级加密托管系统，允许资金在各系统之间流动，在最终接收者收到资金前，传递线路上各个支持Interledger协议的系统会对各环节发送者的资金进行托管锁定。

交易的托管与执行有两种实现模式：原子模式和通用模式。在原子模式中，由参与者选择的一组公证人协调，以确保执行或终止。原子模式通常发生在相互之间可能存在关系的银行或金融服务公司中的受信任连接者之间。通用模式不需要公证人，可以在不受信任的连接者之间工作。它使用 Ripple 公司的内部加密货币 XRP 来促进传输。使用受限的执行窗口对时间进行限制，如果交易没有在一定的时间范围内发生，那么它将被取消。

在公证人机制中，区块链必须信任一组实体（公证人）来做决策，存在一定的安全问题。在不信任一组实体的情况下，哈希锁定可以促进跨链原子操作，从而提供更好的安全性。因此，Interledger在其最新协议中融合了哈希锁定机制。然而，哈希锁定的使用场景仅限于资产交换，并且希望交换资产的用户必须找到另一个链上的合作伙伴，在灵活性方面存在限制。

Interledger 协议在其他项目中也有应用，例如 Hyperledger Quilt 通过Interledger协议（ILP）实现了分类帐系统之间的互操作。

（3） Kepler

Kepler[36]是 VNT Chain 的重要组成部分，由于 VNT Chain 采用的是“联盟链+跨链+公有链”融合的架构，VNT Chain 又称聚合链,。

Kepler Route 跨链技术基于公证人机制，实现了 Hubble Network（VNT Chain 公有链）与 Galileo Network（VNT Chain 联盟链）之间资产的跨链流转与信息的跨链交互。

Kepler 采用事件监听实现跨链价值的快速安全转移，采用重试和超时检验保证交易失败的回滚，并通过与智能合约的交互监控和管理用户账户和跨链交易。基于 Kepler，可以在保持联盟链原有的数据隐私和授权使用特性的同时，获得 Hubble Network 的 token 结算联盟链业务的能力。

（4）Binance（币安）

币安是一个专注于区块链资产流转服务的去中心化交易平台，用于实现数字货币流转。项目实施的愿景在于为资产流通提供安全、公平、开放的平台，并在世界范围内实现区块链资产交易[37]。

基于目前行业中技术架构初级、服务质量低、安全性低以及存在语言障碍等问题，币安致力于提高自身服务平台的性能，保证其安全稳定、高水准服务和多语言支持等特性。此外，币安链也作为一条去中心化的公链，能够开放地创建资产，并且在开发完成后，维护与管理将由全体用户及参与节点进行，以保证其去中心化程度。币安链没有智能合约，也不支持任何图灵完备的语言，主要提供资产上链、货币流通的功能。

除了以上提到的项目之外，Herdius、ReviewChain 等跨链项目也是基于公证人机制。Herdius 使用在 Herdius 中生成的私钥加密用户的私钥（例如，Ethereum 私钥）。然后，使用一种门限多重签名机制，将这个密钥分割并分发给称为汇编节点的公证人。多个汇编节点能够通过组合它们的私钥部分来代表用户签署事务，任何汇编节点都不能完全解密本机私钥。ReviewChain 是一个使用以太坊智能合约的分散审查系统，其中引入了多个区块链网关节点（称为公证人），智能合约和公证人有效地连接了两个不同的基于以太坊的区块链网络。

2. 方案横向对比

下面针对各个项目部分特性进行横向对比。表 3-7 展示了项目基本信息，包括平台、跨链类型、消息验证机制以及签名方案。我们在 2.3.3 节的公证人机制中说明了签名分为中心化/单签名、多签名、分布式签名三种方式，在这里我们对不同项目就签名方案进行对比。

表 3-7 基于公证人的项目间平台、跨链类型、消息验证、签名方案对比

项目名称	平台	跨链类型	消息验证机制	签名方案
Corda	自有链	异构（“类区块链”技术架构）	由一组公证人进行核实	多签名
Ripple	自有链	异构（比特币、以太坊等公有链，私有链，中心化账本和美元等传统支付渠道、超级账本所有开源代码库）	由一组公证人进行核实	多签名
Kepler	自有链	异构（Hubble Network 公有链与 Galileo Network 联盟链）	由一组公证人进行核实	多签名
币安	自有链	异构(比特币、以太坊等，主要是公链)	由单个公证人进行核实	单签名

由表 3-7 可知，虽然均具有跨链解决方案，但各个项目开发均采用独立网络开发方式，而非依赖于现有区块链系统如以太坊等。这种方式可以有效规避现有区块链系统的病弊，针对专门的领域进行更加灵活的设计。签名方案多采用多签名机制，是一种兼顾项目复杂性与安全性的签名机制。

通讯协议列表见表 3-8。AMQP（Advanced Message Queuing Protocol）是一个提供统一消息服务的应用层标准高级消息队列协议，为面向消息的中间件设计。ILP 可以帮助分散式应用程序获取资源，而不受限于特定的区块链网络。ICMP（Internet Control Message Protocol）是 Internet 控制报文协议，用于在 IP 主机、路由器之间传递控制消息；ARP（Address ResolutionProtocol）将 IP 地址转化成物理地址；DHCP（Dynamic Host Configuration Protocol）是动态主机配置协议；FPGA（Field Programmable Gate Array） 是现场可编程门阵列。IPFS（InterPlanetary File System）是一个分布式存储和共享文件的网络传输协议。

表 3-8 基于公证人的项目间通讯协议对比

项目名称	通讯协议	简介
Corda	AMQP	应用层标准协议，包括消息结构、序列化格式、加密方式
Ripple	ILP	系统间支付协议，为 Ripple 提供标准化支付界面的技术，统一 ILP Prepare 等报文格式
Kepler	ARP、ICMP、DHCP 辅助 TCP/IP 协议	用于 FPGA 节点交互，缩短 TCP/IP 堆栈，使 FPGA 处于真实网络中
币安	Origin Protocol	基于以太坊和 IPFS 的去中心化共享经济协议，可以快速高效完成点对点交易

表 3-9 列出了各个项目的共识机制。

表 3-9 基于公证人的项目间共识机制对比

项目名称	共识机制
Corda	公证人节点，BFT-SMaRT，Raft
Ripple	Ripple 协议共识算法
Kepler	其所属主项目 VNT Chain 采用 Vortex 共识算法
币安	BFT 与 dPoS 结合

由于各个项目均为自有链，共识机制均非直接搬用现有的 PoS、PoW 或者拜占庭容错算法等，而是基于现有共识算法的基础上加以改进、或者在应用机制上加以优化，乃至创新性地提出自己的算法，使得项目机制更具有针对性。Corda 由公证人节点提供共识服务，BFT-SMaRT 是通过 BFT 实现状态机复制 SMR（State Machine Replication）的一套改善解决方案，Corda 也通过其他算法如 Raft 等保证交易一致性；Ripple 的协议共识算法 RPCA（The Ripple Protocol cConsensus Algorithm）则基于异步拜占庭容错算法设计；Vortex 融合 DPoS、BFT 与硬件加速，吸取各种方法的特性；币安主要为拜占庭容错（BFT）算法，并与 dPoS 相结合提供共识服务。

表 3-10 中列出了各个项目适用的应用环境。

表 3-10 基于公证人的项目间应用场景对比

项目名称	应用场景
Corda	适用于监管体制下的金融机构，提供资产交易、证券托管等功能
Ripple	跨境支付，跨网络、跨币种的实时国际付款
Kepler	价值流转，专用于实现 VNT Chain 场景互通
币安	区块链资产的交易平台，包括现货交易、杠杆交易等服务

如表 3-10 所示，基于公证人机制的项目主要用于金融领域，为货币流通提供解决方案。Corda 项目早在 2016 年就已经在白皮书中提出项目理念与框架，也是目前较为成熟的金融领域区块链账本技术。Ripple 虽然也可实现金融机构的业务框架，但该项目更主要的愿景是实现全球货币自由交易。其提出的共识

算法 RPCA 与 Interledger Protocol 结合，允许世界各地的银行之间无需中间代理直接进行交易。这种特性使其在跨境货币流通方面备受欢迎。和上面几个项目相比，Kepler 是隶属于 VNT Chain 项目下跨链子项目，其更多是用于 VNT Chain 项目内部的区块链跨链操作。

对项目的特性归纳见表 3-11。

表 3-11 基于公证人的项目间特性对比

项目名称	特性
Corda	1、安全性高，无全局账本与共享机制，只有参与双方能获取交易信息 2、高效准确，公证人节点负责服务共识，保证交易唯一且可信 3、Corda 支持单个交易层上的共识，且共识算法有可插拔特性，交易更灵活
Ripple	1、支持全球无障碍支付，促进世界货币流通 2、交易速度快、延迟低 3、可扩展，理论上可以实现对区块链网络全覆盖
Kepler	1、设计监听机制，保证价值跨链流通的安全可靠 2、基于重试和超时检验策略，回滚失效交易 3、通过与智能合约交互，实现对账户与跨链交易的监控管理。
币安	1、高性能支持，使用内存撮合技术显著提高订单处理速度 2、安全稳定，项目基于多层多集群架构

项目在开发运行过程中也会表现出一些弊端，除了公证人机制本身不能完全实现去中心化的缺陷外，各个项目中也存在一定的限制因素。

表 3-12 基于公证人的项目间限制对比

项目名称	限制
Corda	1、所有交易均禁止全网广播且无 P2P 网络，使其无法承载大规模联盟链 2、系统整体效率较低，且开销不菲
Ripple	1、系统体系倾向于集中化管理方式，通过控制密钥实际上控制账本记录 2、网关体制问题。网关一旦破产，用户手中的虚拟货币则无法变现
Kepler	无相关讨论
币安	1、交易保障能力有限，曾经历数次攻击，造成经济损失

2、不支持法定货币

3.2.3 总结

基于公证人机制实现跨链的项目多是自有链，消息由单个或一组公证人通过单签名或多签名进行核实。项目主要用于金融领域，支持资产交易、价值流转、证券托管等应用场景。使用的共识算法多基于拜占庭容错算法（BFT），常将 BFT 与 PoS 结合。公证人机制较为简单，但是本身不能完全实现去中心化。

3.3 哈希锁定机制

3.3.1 总体概述

哈希锁定技术的核心思想即 HTLC，相比于架构图，流程图更适合于描述哈希锁定的主体思路，如图 3-6 所示[38]。哈希锁定技术在资产互换过程中较好地保证了跨链交易的原子性与一致性，在其基础上实现的项目也在机制或架构方面进行诸多优化，具体项目将在下一节中详细阐述。

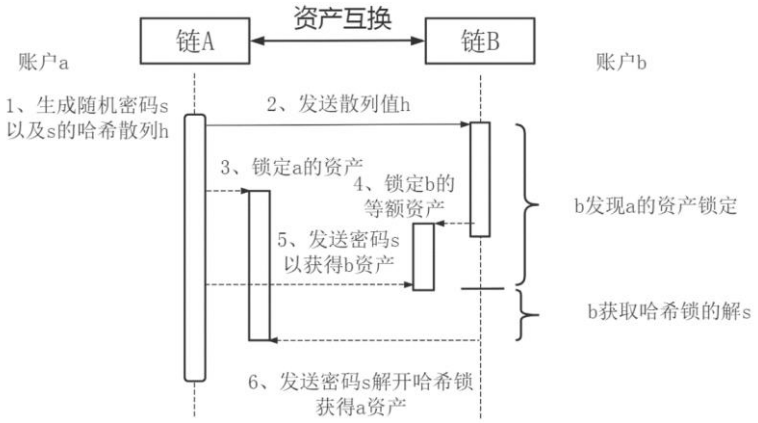

图 3-6：哈希锁定的跨链解决方案图

3.3.2 基于哈希锁定的典型跨链解决方案

1. 方案实例介绍

（1）Lightning Network

闪电网络（Lightning Network）[39]作为一个分布式网络，基于智能合约支持跨链交易和及时交易。闪电网络基于比特币平台搭建，其目的是安全实现链下交易，双方直接通过闪电网络建立的通道进行有效交易。这种方式最大的特性在于免去了以太坊繁琐的上链步骤，缩小交易时间，降低交易成本，适用于高频、快速交易。

闪电网络完成链下交易需要首先建立通道，只有在通道开启与关闭时闪电网络会访问以太坊区块链，期间大量交易数据保存在链下。链下交易失去了分布式账本的安全保障，故闪电网络设计一套完善的惩罚机制，由可撤序列成熟合约 RSMC（Recoverable Sequence Maturity Contract）实现，保障交易的有效性。

但是网络不可能对所有节点建立交易通道，因此闪电网络设计了哈希时间锁合约 HTLC（Hashed TimeLock Contract）用于没有建立通道的两个节点之间进行交易，通过与 RSMC 结合，形成了完善的多中间节点支付通道。

（2）WeCross

WeCross[40]是由微众银行自主研发的开源跨链协作平台，专注于跨地域、跨场景、跨行业的信任传递与商业合作。通过归纳抽象主流区块链的数据结构与资源，使得跨链数据能够以统一的方式进行交互，并进一步探索因多维异构性而无法互通的异构链跨链解决方案。

WeCross 的整体架构分为三层：数据层，交互层和事务层。数据层负责总结归纳不同区块链中的内容；交互层基于上层抽象数据，构建通用区块链适配器与路由中继网络，实现与不同区块链的对接；事务层在此基础上，保证具体场景的跨链事务双方的同时成功或失败。

WeCross 针对行业背景现状与跨链挑战，提出 4S 设计原则。以赋能实体经济为主，可应用于司法跨链仲裁、资产交换等跨链业务，具有广阔的应用空间。目前 WeCross 项目已开源且已投入使用。

（3）Zcash XCAT

Zcash[41]是首个使用零知识证明机制的分布式账本，是密码学技术在区块链上成功应用案例。Zcash 项目参考比特币进行构建，采用 PoW 共识机制，设计上也具有相似性。但 Zcash 的加密方式为零知识简洁非交互式知识论证 zk-SNARKs（Zero-Knowledge Succinct Non-interactive Argument of Knowledge），允许在不泄露交易本身信息的情况下证明交易的真实有效，即实现绝对匿名。Zcash 项目本身的特点也是通过使用零知识证明实现透明与匿名共存的数字加密资产，用户可以选择隐藏交易信息或者在整个网络公开，有助于保护个人隐私。

XCAT 即交叉链原子交易，是 Zcash 与比特币跨链交易工具，本身支持 HTLC，是跨链原子交换技术的应用。目前 Zcash 项目也在尝试建立与 Cosmos 生态系统的互操作性通道，为其带入隐私解决方案。在炼金术项目中则沟通 Zcash 与以太坊，推动零知识证明的应用。

除 Zcash XCAT 之外，Komodo 和 Blocknet 也是原子交换技术的应用。Komodo 继承 Zcash 匿名性，并基于 PoW 独创 dPoW 共识算法保障安全性。

Blocknet 项目通过 XBridge 协议实现节点之间的通信，目的在于建立“区块链互联网”。

2. 方案横向对比

平台、跨链类型与消息验证机制对比见表 3-13，闪电网络基于比特币网络开发，在链下交易时有自己的消息验证方式，WeCross 通过可信事务机制 TTM（Trusted Transaction Mechanism）建立数据互信，Zcash 设计的零知识证明算法在保证隐匿性的同时对交易进行确认。闪电网络沟通比特币与以太坊，WeCross 提出异构链交互协议 HIP（Heterogeneous chain Interconnection Protocol），均具备了异构跨链技术。Zcash XCAT 主要实现了与比特币的互通，且两者技术存在较大的同源性，故将其归为同构跨链。

表 3-13 基于哈希锁定的项目间平台、跨链类型、消息验证对比

项目名称	平台	跨链类型	消息验证机制
Lightning Network	基于 BTC 区块链	异构（ETH，BTC 等）	多重签名技术、RSMC
WeCross	自有链	异构（Fabric 、FISCO BCOS ）	TTM
Zcash XCAT	自有链	同构（ZEC，BTC ）	零知识证明

各个项目通讯协议列表见表 3-14。

表 3-14 基于哈希锁定的项目间通讯协议对比

项目名称	通讯协议	简介
Lightning Network	HTLC	通过散列在节点间传递信息，要求双方在规定的时间内执行合约交易。
WeCross	HIP	主流区块链网络通用协议与交互模式，可连通异构平台
Zcash XCAT	XCAT	比特币与 Zcash 之间跨链交易工具，有效支持 HTLC 技术

共识机制方面，闪电网络在链上提交时基于比特币主链共识，在链下交易时无共识机制。Zcash 采用经典的 PoW 共识完成区块链生成。

表 3-15 基于哈希锁定的项目间共识机制对比

项目名称	共识机制
Lightning Network	链下无，链上基于 BTC 区块链主链共识（PoW）
WeCross	—
Zcash XCAT	PoW

除了闪电网络主要用于金融方面业务实现与处理外，其余项目的应用场景更具多样性。WeCross 基于较先进的跨链技术用于促进多场景信息交流，Zcash 通过其零知识证明可将其隐匿性体现在不同场合中。

表 3-16 基于哈希锁定的项目间应用场景对比

项目名称	应用场景
Lightning Network	即时交易；微支付；跨链支付；外汇套利
WeCross	司法跨域仲裁；物联网跨平台联动；数字资产交换；个体数据跨域授权
Zcash XCAT	数字货币流通；区块链应用开发；执行保密性交易

对项目的特性归纳见表 3-17。

表 3-17 基于哈希锁定的项目间特性对比

项目名称	特性
Lightning Network	1、速度快，大幅提升基于比特币网络的交易速率，几乎瞬间完成。 2、开销小，交易在链下通过闪电网络通道进行，成本低。 3、支持跨链交易，可以快速实现链间汇款，无需其他中介。
WeCross	1、可跨地域部署，架构灵活，根据应用场景可自由定制区块链适配器与资源 2、网络可分层扩展，支持多层次纵深跨链协作 3、可信度高，引入证书颁发机构 CA（ Certificate Authority）身份认证机制，设计多维度的默克尔证明保证可信性
Zcash XCAT	1、有效的隐私保护。采用零知识证明，可以无需公开发送者，金额等交易信息 2、对审计及监管友好。用户可公开地址和交易信息用于审计与监管需要 3、高效可用。可以快速进行网络交易，拥有顶级交易所的支持

对于项目本身也存在一定的限制因素。

表 3-18 基于哈希锁定的项目间限制对比

项目名称	限制
Lightning Network	1、链下通道的建立费用高昂，不适于低频交易 2、当前版本中通道存在资金上限，影响交易性能 3、部分节点会执行大量交易，拥有大量资金，有中心化风险
WeCross	无相关讨论
Zcash XCAT	1、挖矿时的主私钥（ master private key）一旦外泄会造成安全隐患 2、Zcash 筹码过于集中，挖矿和部署过程趋于中心化 3、由于代码开源，社区与基金会、公司的分歧会造成硬分叉

3.3.3 总结

基于哈希锁定实现跨链的项目可以利用哈希的不可逆特性保证数据的完整与安全，验证机制还使用零知识证明、TTM 和多重签名技术等。项目使用的共识机制多基于 PoW。这些项目的应用场景有限，不支持跨链资产转移，资产留置和跨链 Oracle 也存在一定难度。项目具有较好的隐私保护，且快速高效。

3.4 区块链分片机制

3.4.1 总体概述

基于区块链分片的跨链解决方案见图 3-7[42]。分片技术将网络划分为不同的组，每个组都维护自己的分类帐（区块链）并处理和存储不相关的交易集。跨分片通信协议使可以安全地验证原本无法交互的交易并且并行执行。某些分片机制中的节点可以选择参与多个分片的处理并维护其分类帐，某些节点仅参与单个分片。

本节中介绍了四个基于区块链分片的跨链（分片）项目：Ethereum 2.0 Sharding、OmniLedger、Elrond、Rchain。

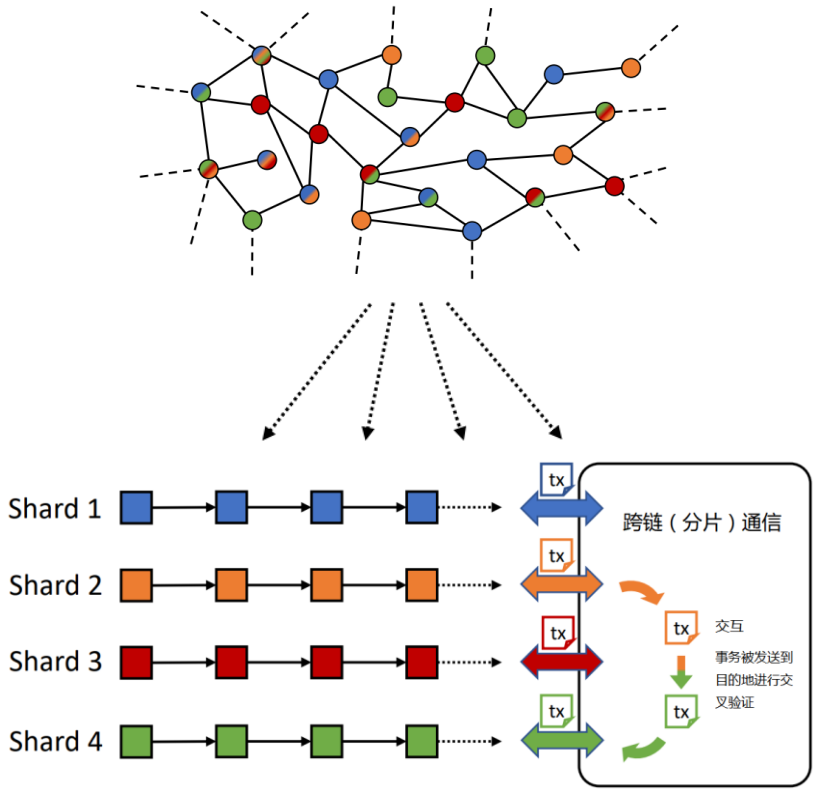

图 3-7：区块链分片的跨链解决方案图

3.4.2 基于区块链分片的典型跨链解决方案

1. 方案实例介绍

（1） Ethereum 2.0 Sharding

Ethereum 1.0 每秒只能处理 7 - 15 个事务，Ethereum 2.0 通过分片实现扩展，将网络的计算需求分片，网络中的节点不必处理（下载、计算、存储和读取）区块链历史上的每一个事务来创建（写和上传）一个新的事务[27]。

以太坊的链上扩容分片技术（Sharding）基于 POS 共识机制，由主链（Main chain），分片链（Shard chain）和信标链（Beacon chain）构成。

在主链（以太坊 1.0，也就是目前正在运行的以太坊）上，分片管理智能合约判断分片中的数据和交易是否为有效的。主链主要是维护验证节点的状态以及跟踪分片链区块状态。

信标链（位于协作层）维护着一个验证者注册表，奖励表现良好的验证者，取消或处罚行为不端的验证者。它每 2-8 秒会生成一个区块，基于随机数生成方法 RANDAO 来分配分片的提议人和验证者。信标链实现了 POS，并为分片方案提供基础。

每个分片链（位于数据层）具有与当前存在的以太坊链相同的容量。分片链主要处理交易以及存储账户、交易信息与合约的状态，并支持跨分片链的消息交互。

分片技术可以实现交易的并行确认，实现链上扩容，提高以太坊的交易吞吐量。此外，不是每个节点都必须处理所有事务，因此分片还增强了可伸缩性。

（2） OmniLedger

OmniLedger[43]由一条身份链（Identity blockchain）和多条子链（Shard）组成。

所有的 Validator 定期根据 RandHound 协议被重新分成不同的组，并随机的将这些组分配到不同的分片子链，进行验证和协商。RandHound 协议需要“Leader”，OmniLedger 使用 VRF 算法来确定“Leader”。Validator 使用 Omnicon 共识确保分片状态的一致性。

OmniLedger 使用称为 Atomix 的拜占庭分片原子确认（Byzantine Shard Atomic Commit）协议来原子化处理跨分片的交易（保证信息的一致性）。它基于分片是集体诚实的、不会无限崩溃的事实，并在内部运行 ByzCoin 拜占庭式共识方案,该方案使用集体签名（CoSi）使 PBFT 更具可扩展性。 该协议是客户端驱动的，分为三个阶段：

a) 初始化阶段，客户创建一个跨分片交易，花费一些输入分片的 UTXO，并在某些输出分片中创建新的 UTXO。交易在网络上流转并最终到达所有输入分片。
b) 锁定阶段，与交易相关联的所有输入分片验证交易，确保输入可以被使用。然后，如果交易有效，则将交易记录在分片的分类帐中，并进行验收证明。 如果交易不被接受，那么将使用拒绝证明。现在已锁定交易输入，但尚未提交交易。客户拥有足够的证据来提交交易或中止交易并收回任何锁定的资金，但不能同时取回两者。
c) 解锁阶段，解锁提交或中止解锁。每个涉及的输出分片都会验证交易，并将其包含在分类账的下一个区块中。交易在第二阶段无效，回滚跨分片交易，并回收交易输入。

（3） Elrond

Elrond[44]提出了一种动态自适应分片机制，能够在事务、数据和网络级别上自适应分片，该机制能够根据需要和活动网络节点的数量进行分片计算和重组。

它通过 SPoS（安全权益证明） 达成共识，随机选择分片内部的节点组成共识组，在共识组中的验证者（Validators ）之间使用修改过的 BLS（Boneh–Lynn–Shacham）多重签名。由于在分片之间周期性地进行节点重组，对恶意攻击具有很强的弹性。每轮重组，每个分片中多达 1/3 的节点将改组为其他分片，以防止串通。BLS 签名和安全随机源，使其具有不可偏向性和不可预测性。Elrond 使用调度算法和路由协议在协议级别上实现了快速确定性（Fast fFinality），在几秒钟内即可完成跨分片交易。

在 Elrond 的跨分片交易中，块结构是由一个包含关于块信息的块头（块随机数、轮次、提议节点、验证节点时间戳等）和一个包含实际交易的每个分片的微块（Miniblock）列表来表示的。每个微块都包含所有事务，这些事务具有在当前分片中的发送方和在另一个分片中的接收方或在其他分片中的发送方和在当前分片中的接收方。微块是跨分片执行中处理的原子单位，在一个块中具有相同发送方和接收方的微块数量没有限制。

Elrond 使用异步模型执行跨分片事务。验证和执行首先在发送方的分片中完成，在公正链中进行公证，然后在接收方的分片中完成。同时，在分片之间平衡智能合约可以使 Elrond 并行运行多个智能合约，跨分片调用也由异步跨分片执行过程处理。

（4） Rchain

Rchain[45]基于名称空间（Namespace）实现分片，名称空间有利于数据的局部性，每个名称空间都是一个区块链，并可以生成次一级的名称空间，最终形成一种树状结构。子分片依赖父分片，子分片的 Validator 可以作为父分片的客户端。

通过智能合约可实现代币在父分片和子分片的转移，父分片中的智能合约叫做 Depository，子分片中的智能合约叫 Mint，Mint 和 Depository 共同建立起父分片和子分片的代币之间的汇率。

跨分片的交易以多级名称空间机制作为基础，在他们的父级分片中处理。由于父级分片存在处理压力的汇聚问题，越是上级的分片对吞吐率的要求越高，RChain 鼓励交易尽量在低层分片解决。

RChain 理论上每秒至少处理 40,000 笔交易，并可以扩展。Casper CBC（Correct-by-Construction）是 RChain 选择实现的 PoS 协议，节点会检查逻辑命

题，但不需要每个全节点都要验证整个区块，CBC 作为一个共识框架，框架内的派生协议保证共识安全性。

除了分片技术和 Casper 协议，Rchain 还融合了 Rho 演算的形式化验证、高并发 RroLang 语言及多虚拟机并行计算技术，具有较好的可扩展性。

2. 方案横向对比

分片是区块链扩容方案之一，除了 Ethereum 2.0 Sharding 是基于以太坊的跨链（跨分片）项目外，其他项目多基于自有链。四个项目都使用了 validators 和签名进行消息验证，但 Validators 的选择和执行内容以及具体的签名方案不尽相同。VRF（Verifiable Random Functions）是可验证随机函数，实现随机数的产生；VDF（Verifiable Delay Functions）是可验证延迟函数；Cosi 是一种可扩展的见证人共同签名协议；BLS 签名由 Boneh、Lynn、Shacham 提出，可以将多个密钥聚合成一把密钥,将多个签名聚合成一个签名。大部分分片链均为同构分片，但也存在异构分片，例如 Rchain 命名空间允许异构部署合同和合同状态；QuarkChain 的子链（分片）具有多样性，QuarkChain 也支持跨分片交易。

表 3-19 基于分片的项目间平台、跨链类型、消息验证对比

项目名称	平台	跨链类型	消息验证机制
Ethereum 2.0 Sharding	基于 ETH 区块链	同构（分片间）	信标链（beacon chain），validators（两类： proposers，attesters），Randao 协议+VDF
OmniLedger	自有链	同构（分片间）	RandHound 和 VRF 算法分配 Validator，集体签名（CoSi）
Elrond	自有链	同构（分片间）	validators 定期重组， BLS 多重签名+VRF
Rchain	自有链	异构（分片间，通过命名空间实现了私有、公共以及联盟可见性所需的组合地址空间）	validators 签名然后把消息发送给父分片，消息需要至少 k 个 validators 的签名

通讯协议见表 3-20。Ethereum 2.0 实现了单向锚定，即燃烧 Ethereum 1.0 的 ETH,然后单向映射,在 Ethereum 2.0 的信标链上生成等量的 BETH。其中 RLPx 是以太坊的底层网络协议套件，包括 P2P 加密通信，节点发现等功能。

表 3-20 基于分片的项目间通讯协议对比

项目名称	通讯协议	简介

Ethereum 2.0 Sharding	receipt paradigm	依赖于一种「朋友的朋友」模式，即验证人可以通过相关联的分片来路由其消息
OmniLedger	Omnicon 协议	将基于组的树通信模式与类似 PBFT 的视图更改过程相结合
Elrond	二进制树	基于二进制树结构的调度机制
Rchain	RLPx 协议	遵循了密切发现和维护已知节点列表的特点，在第一次连接的时候增加了一个二阶段握手协议确保安全通信。通过公钥来交换，并且所有的通信都是加密的。

Casper FFG 是一种混合 POW/POS 的共识机制，Casper CBC 全面转向 POS。但共识机制并不限于 Casper，例如 OmniLedger 就使用了基于 PBFT 的共识，需要注意的是，POW 共识算法不能与分片结合使用。

表 3-21 基于分片的项目间共识机制对比

项目名称	共识机制
Ethereum 2.0 Sharding	Casper FFG+CBC
OmniLedger	ByzCoinX，增强了 ByzCoin 中基于 PBFT 的共识
Elrond	SPOS（安全权益证明）
Rchain	基于 Casper CBC 的 PoS 共识机制

应用场景见表 3-22。

表 3-22 基于分片的项目间应用场景对比

项目名称	应用场景
Ethereum 2.0 Sharding	跨链 Oracle，一个分片上的交易可以触发其他分片上的事件，提升区块链交易处理能力
OmniLedger	跨链 Oracle，提升区块链交易处理能力
Elrond	跨链 Oracle，提升区块链交易处理能力，智能合约的跨链互通
Rchain	资产转移，跨链 Oracle，提升区块链交易处理能力，智能合约的跨链互通

区块链与分片技术结合可以提升交易处理能力，提升交易吞吐量，增强可伸缩性。这些项目都具有更快的交易速度，更低的延迟，且更灵活。

各个项目中也存在一定的限制因素。

表 3-23 基于分片的项目间限制对比

项目名称	限制
Ethereum 2.0 Sharding	1、单分片接管攻击 2、状态转变函数 3、欺诈检测 4、跨片通信 5、数据可用性问题 6、超级二次分片
OmniLedger	1、客户端在这个过程中必须保持运行
Elrond	缺乏相关讨论
Rchain	1、父级分片存在处理压力汇聚问题，级别越高的分片吞吐率要求越高。

3.4.3 总结

基于分片技术并实现跨分片（链）交互的项目多使用验证者（Validator）和签名技术验证消息，同时辅助以 VRF 与 VDF 实现可信随机分片。常用 Casper FFG+CBC 共识机制，也可基于 PBFT 等共识，但是不支持 PoW。应用场景广泛，同时分片技术能够通过并行处理提升交易处理能力，但面临着攻击、欺诈等安全方面的挑战，区块链分片本身也面临着一些技术挑战。

3.5 分布式私钥控制机制

3.5.1 总体概述

分布式私钥控制机制的关键在于私钥分片的管理与跨链等额资产的释放与回收。跨链项目具体实现过程中会在各个方面进行优化与改进，但基本思路如图 3-8 所示，通过分布式私钥管理以实现更高的安全性。

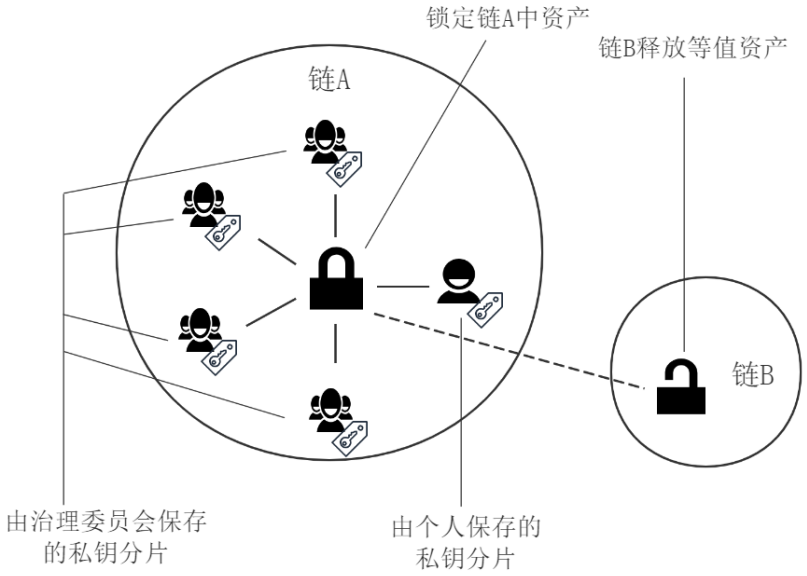

图 3-8：分布式私钥控制的跨链解决方案图

3.5.2 基于分布式私钥控制机制的典型跨链解决方案

1. 方案实例介绍

（1）EKT

EKT[46]定位为一个高性能 DApp 开发平台，用于为开发人员提供一种简单便捷的 DApp 开发方式。同时也作为区块链基础设施，努力开创新型区块链生态系统。

EKT 设计了一套独特的项目架构：多链多共识机制。不同主链间采用不同共识机制，不同的主链拥有不同的主币。因此针对不同的业务可以采用不同的共识机制以保证执行性能，此外由于链间存在数据隔离，事务执行互不影响，保证其安全性。

EKT 项目提供智能合约开发语言 AWM，使得开发者可以根据业务需求定制合约。在扩展性方面，EKT 公链跨链协议允许其他公链资产接入 EKT 主链并自由流通，是连接各个区块链的桥梁。

（2）Fusion

Fusion[47]是一个具有较强包容性，可覆盖各类业务的数字货币金融底链。其愿景是建立加密金融平台级公有链，以实现跨链、跨组织、跨数据源交互，提供完备的金融功能。

Fusion 提出了独有的分布式控制权管理核心技术 DCRM（Distributed Control Rights Management），这种方式从区块链底层密码学实现了资产跨链操

作。Fusion 项目中将资产所有权和控制权的剥离，对资产控制权的转移是基于资产所有权的转移实现。具体流程通过数字资产的 Lock-in（锁定）和 Lock-out（解锁）两个基本步骤完成。锁入时将密钥分片后分布式保管，解锁时验证各分片密钥后，智能合约会在账户中同步更新数据并记录完成情况。

共识机制方面，Fusion 采用计算记账分离方式，计算使用 PoS，记账使用 PoW。综合两种机制特性，有效防止恶意攻击。

（3）Wanchain

Wanchain[48]是连接各去中心化金融场景的基础设施，通过其跨链机制实现不同区块链互联互通，目的在于构建未来分布式银行。Wanchain 项目设计时关注于资产跨链、隐私保护和场景延展等特性，从而保证数字金融与区块链有更大限度的普及。

共识机制方面，Wanchain 基于 PoS 共识设计了新型共识机制，并命名为星系共识。这种机制在随机数生成算法与出块着选择算法上加以创新，具有更高的公平性与安全性。

互操作性方面，万维链设计跨链协议功能模块用于执行跨链协议，具体包括跨链交易数据传输模块和交易状态查询模块，分别主要用于执行跨链交易和跨链查询的功能。Wanchain 作为一个金融底层区块链平台，结合不断落地的 DApp，使其具有相当广阔的应用空间，进而能够有效推广金融区块链在全世界的普及应用。

2. 方案横向对比

平台、跨链类型与验证机制见表 3-24。

表 3-24 基于分布式私钥控制的项目间平台、跨链类型、消息验证对比

项目名称	平台	跨链类型	消息验证机制
EKT	自有链	异构（缺乏信息，跨公链的资产转移）	椭圆曲线数字签名算法
Fusion	自有链	异构（Alprockz，FormulA，Talao 等）	DCRM 分布式签名技术
Wanchain	基于 ETH 区块链	异构（EOS，BTC， ETH，Gemini， Band Protocol 等）	基于椭圆曲线的环签名技术

通讯协议列表见表 3-25。

表 3-25 基于分布式私钥控制的项目间通讯协议对比

项目名称	通讯协议	简介
EKT	EKT 跨公链报文协议	报文协议基于 HTTP 协议以保证兼容大多数公链，有效避免联盟选举的问题
Fusion	Anyswap	基于 Fusion DCRM 技术开发的完全去中心化协议，持基于椭圆曲线数字签名算法（Elliptic Curve Digital Signature Algorithm，ECDSA）或爱德华曲线算法（Edwards Curves Algorithm，EdDSA）任意区块链上的代币置换
Wanchain	万维链跨链通信协议	该协议是其他链与 Wanchain 数据传输规范，通过智能合约实现跨平台资产交换

表 3-26 列出了各个项目的共识机制。

表 3-26 基于分布式私钥控制的项目间共识机制对比

项目名称	共识机制
EKT	默认 DPoS, 不同主链共识机制可以不同
Fusion	PoS 与 PoW 并存机制
Wanchain	星系共识协议（基于 PoS 共识改进）

共识机制方面，均结合应用传统共识如 PoS、PoW 等，使得项目更灵活。EKT 和 Fusion 更多的是在使用机制上加以优化，未对算法本身进行改进。

表 3-27 中列出了各个项目适用的应用环境。

表 3-27 基于分布式私钥控制的项目间应用场景对比

项目名称	应用场景
EKT	电子商务平台；延迟不敏感的游戏； 传统的 Web 应用；社交类的软件；
Fusion	加密金融业务；多币种交互；高拓展性底链
Wanchain	跨链的去中心化交易所；跨链移动支付； 企业联盟链互联；去中心化的金融应用

如表 3-27 所示，EKT 应用场景更宽泛，实现区块链技术在多领域下的普及应用。相比 Fusion 和 Wanchain 均关注于金融领域，其实现思路也大同小异。但

两者主要区别在于 Wanchain 依赖于以太坊构建，定位为分布式银行；Fusion 为独立公链，目的在于实现区块链加密金融服务，因此 Fusion 项目构思与机制相对更复杂，服务更细化。

对项目的特性归纳见表 3-28。

表 3-28 基于分布式私钥控制的项目间特性对比

项目名称	特性
EKT	1、多链多共识机制。不同链内需求采用不同共识算法，兼顾安全性与效率 2、共识效率高，共识算法结合 DPoS 与 Paxos，使得 TPS 不存在理论上限 3、自行设计智能合约：AWM，具有事件驱动, 面向对象, 模块化设计的特性
Fusion	1、DCRM 技术为 Fusion 独创，实现跨链资产管理，保证交易可靠 2、专注于打造数字金融低链，从技术底层改造，有效实现链间交互 3、机制上计算与记账分离，计算使用 PoS，记账用 PoW，防止恶意攻击
Wanchain	1、跨链技术完全去中心化，交易无第三方参与 2、接入时无需修改原有链机制，扩展性高 3、基于密码学机制保证账户交易的安全性与隐私性

各项目限制因素总结见表 3-29。

表 3-29 基于分布式私钥控制的项目间限制对比

项目名称	限制
EKT	无相关讨论
Fusion	1、在互操作性、可扩展性、可用性方面存在挑战，平台性能可以进一步提高 2、项目曾由于黑客攻击导致系统私钥被盗，安全性应进一步保障
Wanchain	1、Storeman 跨链节点组仍存在技术挑战，跨链机制不能完全发挥潜能 2、Wanchain 与 Ethereum 项目具有较高相似度，本身创新性不足

3.5.3 总结

基于分布式私钥控制实现跨链的项目多使用基于椭圆曲线的签名算法验证消息，共识机制均在传统共识（如 PoS、PoW 等）上加以优化。应用场景丰富，支持多币种交互、联盟链互联、去中心化交易所等。分布式私钥控制跨链技术完全去中心化，交易无第三方参与。大部分项目在性能和创新方面仍有待提高。

3.6 其他跨链机制

3.6.1 总体概述

还有很多使用不同于以上提到的跨链机制的方案实现跨链的项目，我们从中挑选出 3 个比较典型的项目进行介绍和对比。

3.6.2 其他跨链机制的典型跨链解决方案

1. 方案实例介绍

（1） NULS

NULS[49]是一个开源的基于微服务的自适应企业级区块链平台，遵循可插拔、模块化和并行扩展的原则，提供智能合约、多链机制和跨链共识。

跨链共识将 NULS 生态系统与外部生态系统和其他区块链连接起来，实现信息和资产的流动循环。NULS 主网采用 POC（Proof of Credit）共识机制和拜占庭容错机制，实现跨链交易的确认和打包，实现分散、高性能和安全性。主网上的每个节点都连接到多个区块链中的多个节点。主网还提供链管理机制来管理在 NULS 主网上注册的所有相等级别的区块链。注册内容包括连锁信息、资产信息、跨链存款等。

当来自其他链的资产被接收到区块链中时，需要在该链中生成相应的资产。不同区块链上的代币以资产形式存储在其他链中。从其他链转移来的区块链中资产的详细信息将存储在 NULS 主网上。当资产从区块链中移出时，将对其进行验证，不允许从区块链中生成非法资产，恶意区块链通过社区机制进行处理，例如暂停跨链、停止跨链、没收存款等。除此以外，NULS 主网为应用程序提供扩展协议，可用于开发 DApp 和优化跨链协议。

（2） ChainLink

ChainLink[50]是去中心化的预言机（Oracle）网络。现有的智能合约无法将数据输出到链外系统，输出通常采用支付消息的形式，路由到用户已经拥有账户的传统中心化的基础设施。ChainLink 允许智能合约连接现实世界的数据、事件和支付，将数据安全地推送到 API 和各种传统系统，ChainLink 可为复杂智能合约提供可靠的防篡改输入和输出。

Oracle 是可用于检索和验证区块链网络和智能合约上的外部数据的程序，使用市场数据源和 Web API 实现。需要向数据源查询特定信息，然后将其连接到区块链。可以创建智能合约来处理从数据源流入的特定信息。Oracle 对于区块链和其他现有平台的功能完全相同。他们从区块链获取查询，在外部平台上查询，然后返回响应。

ChainLink 的链上架构是在以太坊上开发的。智能合约完成了大部分工作，并且在节点内检索数据，提供查询节点需要执行的查询。有三个独特的合约，信誉合约跟踪 Oracle 指标；订单匹配合约根据 SLA（服务等级协议）和智能合约创建者设置的参数从各个节点中获取投标；汇总合约收集节点的答案并为用户的查询提供最终结果，还向信誉合约提供指标。

ChainLink 网络是其链下架构的一部分，它将所有节点连接在一起。 每个节点都通过 API 连接到链下储备，以收集每个合约的响应。所有链下数据都通过 ChainLink 核心软件进行链下转换，以便在链上读取。 分配的子任务也由该软件处理。外部适配器可用于连接到第三方 API 端点，帮助弥合区块链和实际应用程序之间的鸿沟。所有适配器都必须以 ChainLink 的模式格式编写。

（3） Factom

Factom[51]是一种跨链解决方案，同时整合比特币和以太坊区块链，确保数据的安全和可信。通过 Factom，可以将已记录的所有权链“转移”到区块链，但不会受到可扩展性问题的影响，可以在区块链上进行记录保存。

Factom 的作用类似于一个加密的、去中心化且不可变的目录，用一种去中心化的方式来收集、封装和保护数据并锚定到比特币或以太坊。锚定为 Factom 区块链提供了增强的安全性和跨链互操作性。

通过在其他区块链中插入加密锚，增加了抵抗攻击的几率——要使攻击成功，需要在 Factom 区块链锚定的所有区块链上均取得成功。同时，回滚 Factom 区块链需要同时回滚其他几个区块链。

随着 Factom 区块链定期将其数据的 Merkle 根证明插入其他链中，它创建了一条从一个链到另一个链追溯证明的路径。锚定到其他区块链可以跟踪 Merkle 根到最终锚点。如果数据已更改，则附加区块链中的哈希将不匹配。

2. 方案横向对比

由于他们使用的并不是同种共识，想要解决的问题也并不相同，本文首先对他们的目的/着眼点进行了比较。

表 3-30 项目间目的/着眼点对比

项目名称	目的/着眼点
NULS	定义了一套跨链通信协议
ChainLink	解决链上链下的数据流通问题
Factom	收集、封装和保护数据并锚定，类似于一个目录

三个项目都使用了多种验证方式确保消息的正确性。NULS 使用了分布式验证，结合了 POC 共识机制和拜占庭算法实现共识节点拜占庭签名，并且计算接受和转出的资产总和进行链资产验证以隔离链安全风险。ChainLink 使用了可验证随机函数和门限签名确定链下数据源的真实性。Factom 让用户客户端和应用程序来执行大多数的数据验证任务，需要定义协议中的交易并建立一个链来保存交易。

表 3-31 项目间平台、跨链类型、消息验证对比

项目名称	平台	跨链类型	消息验证机制
NULS	可与 BTC/ETH 对接	异构（比特币、以太坊等）	分布式验证、共识节点拜占庭签名、链资产验证
ChainLink	基于 ETH 区块链	异构（链上链下）	可验证随机函数（Chainlink VRF）、门限签名
Factom	可以兼容 BTC 和 ETH	异构（比特币、以太坊等）	客户端自定义的记录链（Chains of Entries）

该类涉及的跨链项目通讯协议多为自定义的，如下表 3-32 所示。

表 3-32 项目间通讯协议对比

项目名称	通讯协议	简介
NULS	NULS 自定义、开放的协议	NULS 定义了一套跨链通信协议，包括：链间网络连接维护、链间交易推送、链间交易验证、链间数据查询，且协议本身是开放的。
ChainLink	去中心化的预言机网络	功能上相当于 HTTP 协议（可信执行环境中相当于 HTTPS）,实现链上和链下的协议层和应用层信息传输。
Factom	Factom 协议	独立节点通过 Factom 协议与比特币/以太坊通信。Factom 充当一个加密的、不可变的目录，而不是在区块链上存储整个记录。

三个项目的共识机制，有的是多种机制的结合；有的是对一种基础的共识机制进行改进，例如 Factom，只有已经提交到系统的权益有投票权，而可转移

的 Factoid 权益没有投票权，避免了 POS 机制的“股份磨损”和“没有人进行 POS”问题。

表 3-33 项目间共识机制对比

项目名称	共识机制
NULS	POC（Proof-Of-Credit，信用共识机制）+共识节点拜占庭签名
ChainLink	链下（去中心化 oracle 网络）
Factom	POS 改进

应用场景归纳见表 3-34。

表 3-34 项目间应用场景对比

项目名称	应用场景
NULS	跨链资产转移
ChainLink	证券智能合约、保险智能合约、贸易融资智能合约，可用于确认合约义务的履行
Factom	在区块链上建立不可更改的审计公证业务流程，记录保存

各项目的特性对比如下表 3-35 所示。

表 3-35 项目间特性对比

项目名称	特性
NULS	1、公开的简单的跨链协议；2、去中心化程度更好；3、通过 POC 和拜占庭算法保证交易的安全性，在资产上做到风险隔离；4、解决很多区块链项目的重复工作；5、多资产跨链，每个链都可以登记任意种资产；6、业务跨链；7、账户协议可以降低私钥维护难度
ChainLink	1、解决智能合约的连通性问题：使智能合约能够连接任意外部 API 2、区块链中间件链接链下世界：将各个网络中的智能合约连接，整合关键功能；通过智能合约连接链下数据，连通外部事件 3、保证智能合约端到端的可靠性：提供连接外部数据的可靠解决方案
Factom	速度更快，更便宜，且不会造成区块链膨胀。

各个项目中也存在一定的限制因素，见表 3-36。

表 3-36 项目间限制对比

项目名称	限制
NULS	1、开发进度慢 2、NULS 代币曾被盗，原因是 NULS 交易签名验证逻辑存在一个 BUG，现已硬分叉
ChainLink	1、成本问题，多个 Oracle 聚合时成本较高 2、请求响应模式有一定的延迟，从请求发出到数据写回通常需要经过几个区块的间隔 3、资源浪费，不同的客户端请求同一个数据会造成同一数据重复写入区块
Factom	在 Factom 中对数据进行更改、修改、重新排序或删除很困难

3.7 本章小结

本章从所选择的多个典型的区块链跨链项目出发，详细说明每个项目的技术细节，也为下一章高维度的分析讨论提供案例支持。本章节介绍了侧链/中继、公证人、哈希锁定、区块链分片、分布式私钥控制五种不同的跨链机制分类，并深入剖析了各分类的跨链支持项目以及其他未明确分类的典型跨链项目。本文从项目支持平台、消息验证机制、通讯协议、共识机制、应用场景、特性和限制等方面展开横向对比，来全面展示现有跨链技术方案如何依赖并实现不同的机制以应对区块链的互操作性需求（研究问题 2）。

第4章 进一步讨论

本文上一章节分析了所发现的跨链技术解决方案现状，并从不同的角度对比了各跨链机制下典型项目的特点。本节将从跨链机制层面就技术和非技术角度展开进一步的分析对比，并讨论现有跨链技术解决方案的难点和未来的应对方向，以回答研究问题 3。

4.1 跨链机制间对比分析

4.1.1 技术性对比

五种典型的跨链技术对比如表 4-1 所示，表格参考了路爱同等人的跨链机制性能对比分析[11,12]以及第 3 章的项目结果。其中，拓扑结构反映了链与链互操作的方向与对应关系，N 表示任意数量的区块链，1 表示一个区块链，C 表示一个连接器实体（例如，一个公证人）。信任模型用于建立信任关系。验证机制用于证明一笔交易是真实有效的。跨链实现/应用的对比与 2.3.1 节的跨链目标有关，同时，它也一定程度上影响了应用领域范围，例如，如果该方案不支持资产转移，那么在股票、债券、金融衍生品市场上的一些应用是很困难的。

表 4-1 跨链机制间技术对比

	公证人	侧链/中继	分布式私钥控制	哈希锁定	分片
简述	由一组可信节点作为公证人，向区块链 X 证明某一特定事件是否发生在区块链 Y 上	侧链基于锚定在某个区块链上的 Token/在链间建立中继链	用户与去中心化网络共同管理私钥，不存在第三方	通过锁定一段时间来猜测哈希值的明文	由主链和分片（shards）链组成，一个分片对于共同访问的状态的修改，需要及时地让另一个分片知道
通信	双向通信	one-way peg 单向通信，two-way peg 双向通信	双向通信	双向通信	one-way peg 单向通信，two-way peg 双向通信
拓扑结构	N←→C←→N	1→1 或 N←→N	N←→N	N←→N	N←→N
信任模型	大多数公证人诚实	链不会失败或者受到“51%攻击”	链不会失败或者受到“51%攻击”	链不会失败或者受到“51%攻击”	链不会失败或者受到“51%攻击”
验证机制	由单个或一组公证人进行验证	常用 SPV，也使用验证者（validator）、半信任第三方等	多使用基于椭圆曲线的签名算法，也使用零知识证明、分布式门限签名等技术	哈希算法，同时辅助以零知识证明、TTM（可信事务机制）和多	验证者（validator，基于不同算法分配或重组）和签名技术（CoSi，BLS

					重签名技术等	等），辅助以 VRF 与 VDF
共识机制或容错机制		多基于拜占庭容错算法（BFT），常将 BFT 与 PoS 结合，或基于 BFT 改进	多种，PoW，PBFT，GRANDPA，共识算法插件等	多基于 PoS，或 PoS 和其他共识机制共存或结合	多基于 PoW	多采用 Casper FFG 和 Casper CBC，也可基于 PBFT 等，但是不支持 PoW
跨链实现/应用	跨链交换	支持	支持	支持	支持	支持
	跨链资产转移	支持（需要长期公证人信任）	支持	支持	不支持	支持
	跨链 Oracle	支持	支持	支持	不直接支持	支持
	跨链资产留置	支持（需要长期公证人信任）	支持	支持	大多数支持但有难度	支持
	跨链智能合约	困难	困难	支持	不支持	部分支持
实现难度		一般	困难	一般	容易	困难

本文通过阅读相关项目的文档和学术论文，汇总了所涉及跨链方案的优点和缺点，具体如下表 4-2 所示。

表 4-2 跨链机制间优缺点对比

	公证人	侧链/中继	分布式私钥控制	哈希锁定	分片
优点	最简单的跨链互操作方案	平衡了可扩展性、安全性及性能。满足的跨链应用场景较多	用户与去中心化网络共同掌管私钥，交易无第三方参与	链与链之间不用或尽可能少的了解彼此，提高了交易的速度。	并行处理事务提升了效率，减少计算或存储的冗余，一定程度上保证了非中心化，理论上能够无限扩展
缺点	采取集中化管理方式，一定程度上不符合区块链的去中心化理念	有的仅为单向通信，应用有局限性。中继链压力较大，结构复杂	智能合约方面还有待加强，实现更多的功能	不支持资产转移和跨链智能合约，实现跨链 Oracle 和资产留置也存在一定难度，应用场景受限，适用性低	作恶成本相对降低，安全风险较高，目前仍存在一系列技术难题有待解决

4.1.2 非技术性对比

本文调研了并对比分析了从不同跨链机制的非技术性属性，结果涉及了安全、通用性和可扩展性、原子性、交易速度以及去中心化程度等属性。

（1）安全

公证人机制使用公证人互信确保网络安全，单签名即中心化公证人的安全性最为脆弱，分布式或多签名的安全性相对较高。由于依赖于公证人的诚实性，虽然多签名使用了随机、定期重组等选举策略，但依赖并未完全消失，存在一定的风险。侧链/中继链使用 Merkel 证明等技术实现跨链安全交易，可以实现快

速的完整性验证，但无法像主链全节点一样实现全面的验证。侧链也在一定程度上保障了安全，侧链上出现漏洞，主链不会受到影响。哈希锁定机制中使用了哈希锁与时间锁保证安全，但交易阻塞超时可能会导致安全问题。分布式私钥控制使用多签名算法保证跨链交易安全性。分片的安全性较为脆弱，单分片受到攻击可能会影响其他分片。此外，由于区块链依赖于矿工的诚实，链失败或者受到“51%攻击”会存在一定风险。

（2）通用性和可扩展性

通用性方面，公证人机制由公证人决定支持的平台类型，侧链/中继机制由侧链/中继链决定。基于分布式私钥控制的项目的底层链需要支持脚本和签名校验。基于哈希锁定的项目有的支持比特币，有的支持以太坊。分片与跨分片交互是以太坊 2.0 的主要目标，虽然比特币等平台缺少分片技术的应用研究，但 Quarkchain、Elrond 等知名公链也使用了分片技术。

可扩展性方面，公证人机制由公证人决定，而侧链与分片技术本身均是区块链扩展的技术主流，侧链是主链外的另一个区块链，而分片则是将区块链进行内部分割。哈希锁定机制和分布式私钥控制机制也支持平行扩展。

（3）原子性

不同跨链机制实现原子性的原理不同，公证人机制的交易原子性由公证人担保；侧链/中继机制的原子性则由合约实现；哈希锁定机制通过哈希锁定算法和超时机制确保交易的原子性；分布式私钥控制机制则由多签名算法保证；跨分片的原子交易需要分片之间同步通信的验证者。

（4）交易速度

公证人机制的交易速度较慢。侧链/中继链机制允许小额交易在侧链上完成，既加快了交易速度，又减轻了主网的压力。哈希锁定机制减少了链与链之间的相互了解的需要，并且通常会和“状态通道”（State channel）搭配，提高了交易速度。分片技术能够并行处理事务，但是交易速度的增长受限于当前可以在隔离的分片中同时执行的交易数量（即受交易串行化影响）。

（5）去中心化程度

公证人机制的去中心化程度较低，特别是单签名公证人。侧链/中继链可以实现数据去中心化并且并行处理，但单一托管模式和联盟模式实现双向锚定存在一定的中心化，并且联合挖矿可能会带来挖矿中心化。分布式私钥控制将私钥分成多处保管，去中心化程度较高。哈希时间锁允许以去中心化、无需受信任第三方的方式进行条件支付。分片技术也有助于网络去中心化。

4.2 跨链技术难点与解决方案

区块链的跨链技术作为一种新兴的技术方向正在快速发展，但目前尚未有一种统一机制真正完成“全球链联网”的构想，目前跨链技术发展仍面临不少技术挑战亟待解决。本次调研从 103 个跨链项目中选取了 39 项有效数据，对其暴露出的难点与局限进行归类统计，共总结出 4 个技术挑战点，分别为下文（1）~（4），统计见图 4-1。

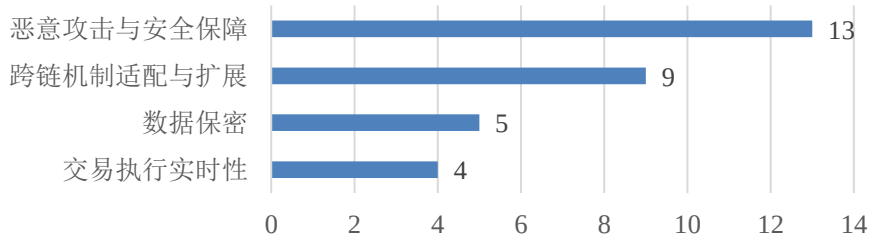

图 4-1：各技术难点数量统计

此外，通过对十余篇跨链技术综述与二级研究调查分析，归纳出跨链技术中最关键的 3 个问题，分别对应下文（5）~（8）。下面将分别进行阐述：

（1）恶意攻击与安全保障

安全性问题一直是区块链系统关注的焦点，主要包括跨链原理与机制本身的安全缺陷和区块链结构特点造成的安全隐患。在跨链交易过程中，如果跨链交易遭受攻击，会牵连整个跨链网络结构，造成更严重的后果。恶意攻击问题是各个项目中提及最频繁的一个问题，而且也是最难解决的问题。因此需要构建严密的安全保障机制，最大限度保障交易安全。在调查过程中，Fusion、币安、NULS 均出现过恶意攻击案例，导致经济损失，PalletOne[52]的 DAG 技术也有一定的安全风险，易受双花攻击。

安全性保障问题亟待解决，虽然攻击方式多样，但可以从如下几个方面提供研究参考：1、对于存在中继器或跨链网关的机制，中继节点应有安全监测与响应能力，具有类似防火墙的功能[11]。中继节点安全功能的开发有待进一步研究。2、应对网络结构导致的问题如网络超时等，可以设立相应的安全检查点，时刻监测网络运行情况，避免恶意阻塞[6]。3、针对网络内部恶意节点，如矿工劫持挖矿，即矿工恶意占用用户算力、内存等资源等行为，需要有相应的反劫持机制和策略以保护普通用户[53]。4、完善对意外事故的预防能力和补救方案。虽然目前对跨链方案安全性有基本考虑，但仍需进一步深入研究，如对跨链交易过程中恶意操作及时识别，以及对于已发生问题提供完善有效的补救措施等。

（2）跨链机制适配与扩展

跨链项目最主要的关注点就是跨链机制的适配与扩展，主要包括对现有区块链的交互情况和对后续改进的未来区块链兼容情况。链间扩展，特别是异构链间的链接具有一定挑战[13]。BTC Relay 只支持比特币与以太坊的互通，缺乏通用的适配性，AION 项目[54]对接入主网的区块链网络要求进行改造，Mimblewimble 项目[55]提出很难以向后兼容的方式引入比特币网络。拥有高适配性的网络更容易与外部网络对接，从而更好支持跨链交易甚至多跳跨链通信[12]。

在提高适配性与扩展性方面，主要有两种解决思路。1、对于现有区块链系统，可以主动的设计专用接入接口或通信协议，实现对外部区块链的一一对接。由于是专用接口，实现更具针对性。但其通用性不足，难以应对未来日益增加的异构区块链系统。2、对于尚未开发的区块链系统，可以从底层切入。开发底层跨链基础设施或通用的跨链通信协议，实现简洁安全的跨链对接。这种方式应用范围广，适合未来复杂多变的应用环境。目前主流跨链项目如 Cosmos、Polkadot 等均采用这种理念进行设计与尝试。但底层平台一般机制复杂，兼容性要求高，有一定技术挑战，底层跨链平台的优化与完善也是许多研究机构关注的问题之一[7,11,56]。

（3）数据保密

良好的数据保密措施将有助于保障用户个人隐私信息，在跨链交易中泄露隐私如资产数据、个人私钥等内容会导致严重后果，更容易遭受黑客恶意攻击[57]。InterChain[58]在白皮书中介绍应进一步隐藏跨链细节以防止恶意篡改；Zcash XCAT 也考虑到存在私钥外泄而导致的安全隐患。

对于解决跨链隐私保障问题，有几种思路可供参考：1、设置交易接口[9]。接口的设计可以从较底层的跨链协议或跨链共识上实现，也可以在跨链智能合约中选择性地发送交易数据。2、基于密码学算法[59-61]，如环签名技术、同态加密、零知识证明技术等。其中零知识证明技术已经在 Zcash 得以实践并取得一定成果，实现匿名交易。环签名技术也在许多项目中得以应用，用于保护用户个人隐私信息。可以通过对密码学技术与区块链网络的结合研究，探索更具优势的隐私保护机制。3、类比 Corda 项目实施选择性共享，交易细节仅可由交易双方获取。由于 Corda 禁止全网广播且无 P2P 网络，其技术实现难以支撑大规模网络。可以考虑对选择性共享策略加以改进，扩大其应用范围。

（4）交易执行实时性

许多交易有着严格的时间要求，然而区块链系统交易普遍存在延迟，尤其是跨链交易情况会更加严峻，无法满足立即支付交易的需求。过长的交易时间

使得整个区块链系统难以步入日常服务中，大幅限制了其应用范围。比特币平均确认时间在十分钟左右；Comit 项目[62]也表示无法支持速度要求高的交易；ChainLink 的请求响应模式存在一定的时间延迟，实时性低。

在解决交易速度方面，可以参考已有项目并在其基础上加以改进。1、闪电网络通过建立链下交易通道免去繁琐的上链步骤，大幅提高吞吐量，实现快速交易。但关于通道建立的开销以及对已有通道复用优化的问题需要进一步解决。2、BOS 通过 Batch-PBFT 共识机制将区块链出块和共识消息分离，每次广播多个块的信息，实现秒级交易[63]。但该技术对于跨链交易尚未得到应用，跨链秒级交易有待实现。3、还有一些其他解决方案：如直接增大区块容量；这种方式对网络要求高，可行性较低。还可以进行小团体的代理人共识，在小范围内进行交易确认，提高验证速度；但其交易透明性与安全性有待考量。

（5）跨链信任的传递

跨链信任的传递即跨链信息的有效性证明[11]。目标链需要验证源链的跨链交易是否有效，确保其不会发生转移冻结资产、资产双花现象以及源链和目标链资产状态不一致等情况。由于区块链之间存在数据隔离，一般不会与外界进行主动的信息交互，因此验证外部链上的交易成为所有跨链解决方案需要面临的难点之一。目前，跨链交易的真实性和有效性验证一般分成三个阶段：跨链数据传输、源链交易确认和目标链对已确认交易的验证[64]。

在解决跨链信任传递问题上，普遍的方法是引入一个“中间人”。“中间人”会负责链间信息的收集与传递。而根据对链间信息确认方式与确认地点的不同，区分出公证人机制和侧链/中继等技术。公证人机制下交易验证均由可靠的第三方节点进行。侧链/中继机制中“中间人”只负责传递交易信息，跨链信息会保存在区块链各自的网络中，并根据 SPV 机制独立进行交易验证。两种机制各有利弊，但就当下而言侧链技术应用更加广泛[56]。如何进一步简化跨链信任传递流程，实现跨链事务快速高效证明值得进一步探索实践。

（6）跨链交易的原子性、一致性

交易原子性指一次交易或者完全成功执行，或者完全不执行，不存在中间状态。一致性指跨链网络中不同链间在交易后存储数据与其他信息的最终状态一致。通常跨链交易不是一个单纯的事务，而是由多个步骤集成，因此在两个乃至多个链间保证一次交易的原子性与一致性并非易事，目前对相关方面已有一定的讨论[10,11,13,56,64,65]。不同链之间共识机制、验证方式、底层结构等往往大相近庭，往往导致交易无法最终完成。交易状态的其他因素还有有很多，常见

的包括网络阻塞、节点延迟、恶意攻击等。保证跨链交易的原子性与一致性、实现链间事务性管理是跨链技术一大难题。

在解决交易原子性问题上最初方案为跨链原子交换技术，后来演变为HTLC，成为哈希锁定技术的基础。在此之上进一步泛化出现 HTLA，因其更具普适性，可以通过引入至其他跨链项目中保证跨链交易原子性[56]。在一致性上可行的方案有区块纠缠、使用 DPoS/xBFT 等共识算法。区块纠缠在不同链的区块之间建立联系，但这种方式耦合度较高，难以大范围应用。DPoS 等共识从算法角度上改进，相比 PoW 更高效、更容易达成交易的最终一致性[66]。目前跨链交易原子性与一致性尚未完全解决，需要更加可靠有效的对应方案以实现更复杂环境下的交易事务性管理。

（7）跨链前后的资产总量恒定

跨链资产互换与货币汇率兑换类似，总价值量在交易前后保持一致。资产互换的本质是两条链上价值相同的资产同时交换了持有人，每条链上资产总量不变[64]。保证总量不变的必要前提是对资产的锁定与解锁[11]。正常情况下，引发资产总量变动的原因包括网络故障、节点宕机等，而往往保证跨链交易的原子性、一致性以及跨链交易的真实有效即可避免发生资产总量不一致的现象。但在异常情况下，如跨链交易后参与交易的某个链发生重构、分叉或数据丢失等意外，跨链价值难以保证一致。

保证资产总量恒定首先要保证交易的真实性与事务性，即前两小节提到的问题。对于异常情况下，可行思路是隔离异常链，并拒绝接受所有该链上的交易请求直至问题解决为止。或者对于异常情况导致的异常交易及时冻结，直至异常恢复[56]。由于异常情况发生概率低，且跨链技术目前仍然不够成熟与完善，没有针对诸如区块链重构等小概率情形更有效的对应方案，有待做进一步研究。

（8）区块链跨链系统性能

跨链系统的性能更多依赖于参与跨链的区块链本身的性能指标，而目前区块链性能仍普遍有待提高，诸多问题有待进一步探索解决，如：在高并发下如何提高区块链吞吐量，如何提高区块链分片技术中分片机制的可靠性与跨分片通信能力等等[43,67,68]。

可以通过更加科学化系统化的方法实现对高性能区块链系统的认知与对当下区块链系统的优化方式[53]。如：1、通过排队论对事务处理、区块生成等排队相关的流程进行建模优化，提高系统性能。2、通过设计优先级服务策略以实现对安全性与规范性的预期。3、通过通用的概率模型描述各性能指标间的相关性并进行优化。

此外，还有一些研究方向可作为提高系统性能的参考：1、区块链大多基于 P2P 网络，可以对网络中的 mac 层、路由层等部分进行性能优化以确保数据高效传输。2、通过先进硬件辅助，对一些关键节点如矿工节点等加速数据访问。3、对于多链并行挖矿机制，通过跨链协议实现全局区块生成与管理。

4.3 本章小结

确定合理的跨链方案选型是跨链实现的一个重要部分。本章节通过对跨链项目的提炼总结，详细对比不同跨链机制间的技术性和非技术性区别，并且统计项目中提到的技术难点，列出可能的研究方向或解决思路。

在前几章中，我们的见解和发现是较为分散的，在本章节，我们提供了模式及功能之间的整体比较，归纳了跨链技术发展中相对普遍的技术难点与解决方案，可供相关研究者或实践者做进一步研究与探索。

第5章 总结展望

区块链技术在不断发展与完善，其交易性能、安全性与治理机制均日趋成熟，应用领域不断拓宽，不同行业下的区块链项目也如同雨后春笋一般不断快速涌现与发展。因此，在区块链 3.0 时代下，“区块链孤岛”将越来越多，跨链技术的重要性也得以体现。跨链的发展不仅仅是区块链技术自身在未来演化的必然趋势，更是各行各业日益关注的需求，是构建全球链联网的核心。

本文基于当下主流跨链机制，在学术期刊与网络检索中收集整合跨链项目相关资料，详细展示出各个机制下典型区块链跨链项目。通过各机制间以及各项目间的对比寻找共性、分析特性，总结出不同类型项目的优势与局限、区块链平台开发性能关注点以及跨链技术难点和可能的解决方案，旨在帮助了解区块链技术的发展现状和发掘未来关于该技术的研究方向。

我们通过本次调研取得一定的结果：1、系统整理了跨链方案，展示出跨链技术必要背景和发展现状。2、通过对跨链解决方案进行分析与对比，为跨链技术的实践与研究奠定基础。3、讨论了目前跨链解决方案面临的难点与解决方案，为跨链技术进一步发展提供可参考的研究方向与思路。目前跨链技术仍处于研究的初级阶段，其探索与应用均具有相当的复杂性与挑战性，因而更需要多方齐心协力，共同推动跨链技术发展，构建全球区块链互通体系。

综合前文，本次研究工作在项目落地实践与区块链技术研究方面具有一定的实际意义：

对于实践者而言，可以根据各个项目与机制间对比，针对不同的应用场景确定开发技术选型、优化项目治理方式。文章 4.1 节总结开发过程中的项目属性，并结合各个机制进行讨论，开发者可以依此对区块链项目性能进行评估与优化，综合安全性、通用性、原子性、交易速度与去中心化程度等方面保障系统高效稳定运行。4.2 节列出了一些可能遇到的技术难点，开发人员可以妥善应对、防患未然。同时，根据实际开发与运维经验，努力寻找应对技术难点的可行方案。

对于研究者而言，可以考虑如何结合各机制与项目的优点进一步优化各个性能指标，确保交易更安全、更快速，链间通信更便捷、更统一，进而使得区块链系统更具普适性。此外，针对 4.2 节列出的问题，研究者们可以寻找优化的解决方案，如：寻找能够提高安全性的通用方式以有效防范多种恶意攻击；提高跨链机制适配性，或设计一种能够沟通多种异构链的统一跨链协议；提高区块链中用户私人信息与交易数据的保密性，保障隐私性；保证交易实时性，实现跨链交易秒级处理等。

跨链技术是实现地域区块链互连甚至全球价值流动互通的关键。在未来将会有更多的应用场景建立区块链平台，也会有更多的科研领域引入区块链技术，跨链技术将带来跨领域、跨学科的场景融合，推动交叉学科与前沿科技的发展。区块链互操作性的优化与完善也会为云计算、物联网等技术带来更大的发展空间，有效解决信息传输与价值交换的安全性与可信度的问题，加速推动社会进入万链归一，万物互连的新时代。

参考文献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[R]. Manubot, 2019.

[2] Xu B, Luthra D, Cole Z, et al. EOS: An architectural, performance, and economic analysis[J]. Retrieved June, 2018, 11: 2019.

[3] Advanced Decentralized Blockchain Platform[EB/OL]. https://tron.network/static/doc/white_paper_v_2_0.pdf.

[4] 高志豪. 区块链之跨链技术介绍[J]. 金卡工程, 2016, 000(011): 46-51.

[5] Blockchain Interoperability: Cosmos vs. Polkadot[EB/OL]. https://medium.com/@davekaj/blockchain-interoperability-cosmos-vs-polkadot-48097d54d2e2.

[6] 李芳, Fang L, 李卓然, et al. 区块链跨链技术进展研究[J]. 软件学报, 2019, Vol.30Issue(6): 1649-1660.

[7] Jin H, Dai X, Xiao J. Towards a novel architecture for enabling interoperability amongst multiple blockchains[C]. 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), 2018: 1203-1211.

[8] Deng L, Chen H, Zeng J, et al. Research on cross-chain technology based on sidechain and hash-locking[C]. International Conference on Edge Computing, 2018: 144-151.

[9] Hegnauer T. Design and Development of a Blockchain Interoperability API[D]. Master's thesis, CSG@ IFI, University of Zurich, Switzerland, to appear 2019 …, 2019.

[10] Miraz M H, Donald D C. Atomic cross-chain swaps: development, trajectory and potential of non-monetary digital token swap facilities[J]. Annals of Emerging Technologies in Computing (AETiC) Vol, 2019, 3.

[11] 路爱同, 赵阔, 杨晶莹, et al. 区块链跨链技术研究[J]. 信息网络安全, 2019, 19(8): 83-90.

[12] Kannengießer N, Pfister M, Greulich M, et al. Bridges between islands: Cross-chain technology for distributed ledger technology[C]. Proceedings of the 53rd Hawaii International Conference on System Sciences, 2020.

[13] Qasse I A, Abu Talib M, Nasir Q. Inter Blockchain Communication: A Survey[C]. Proceedings of the ArabWIC 6th Annual International Conference Research Track, 2019: 1-6.

[14] Robinson P. Consensus for Crosschain Communications[J]. arXiv preprint arXiv:2004.09494, 2020.

[15] 区块链服务网络发展联盟. 区块链服务网络用户手册[J], 2020.

[16] 中国信息通信研究院. 可信区块链推进计划. 区块链互操作白皮书（1.0 版）[R]. 2020.

[17] 程婧斐. 基于区块链技术的共享经济应用研究[D]. 北京邮电大学.

[18] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.

[19] 邵奇峰, 金澈清, 张召, et al. 区块链技术:架构及进展[J]. 计算机学报, 2018, 041(5): 969-988.

[20] Yuan Y, Wang F Y. Blockchain and Cryptocurrencies: Model, Techniques, and Applications[J]. IEEE Transactions on Systems, Man, and Cybernetics, 2018, 48(9): 1421-1428.

[21] 王晓光. 区块链技术共识算法综述[J]. 信息与电脑, 2017, (9): 72-74.

[22] 贺海武, 延安, 陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展, 2018, 55(11): 112-126.
[23] Buterin V. What is Ethereum?[J]. Ethereum Official webpage. Available: http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html, 2016.
[24] Dhillon V, Metcalf D, Hooper M: The hyperledger project, Blockchain enabled applications: Springer, 2017: 139-149.
[25] Greenspan G. Multichain private blockchain-white paper[J]. URl: http://www.multichain.com/download/MultiChain-White-Paper.pdf, 2015.
[26] Buterin V. Chain interoperability[J]. R3 Research Paper, 2016.
[27] Wels S J. Guaranteed-TX : The exploration of a guaranteed cross-shard transaction execution protocol for Ethereum 2.0, 2019.
[28] BTC Relay's documentation.[EB/OL]. http://btc-relay.readthedocs.io/en/latest/.
[29] Kwon J, Buchman E. Cosmos: A network of distributed ledgers[J]. URL https://cosmos. network/whitepaper, 2016.
[30] Wood G. Polkadot: Vision for a heterogeneous multi-chain framework[R]. White Paper, 2016.
[31] Lerner S D. RSK White paper overview, 2015.
[32] 叶少杰, 汪小益, 徐才巢, et al. BitXHub: 基于侧链中继的异构区块链互操作平台[J]. 计算机科学 47(6): 294-302.
[33] Jiang Y, Wang C, Wang Y, et al. A cross-chain solution to integrating multiple blockchains for IoT data management[J]. Sensors, 2019, 19(9): 2042.
[34] Hearn M. Corda: A distributed ledger[J]. Corda Technical White Paper, 2016, 2016.
[35] Thomas S, Schwartz E. A protocol for interledger payments[J]. URL https://interledger. org/interledger. pdf, 2015.
[36] KEPLER [EB/OL]. https://github.com/vntchain/kepler.
[37] Binance 白皮书[EB/OL]. https://www.chainnode.com/doc/3482.
[38] 关于跨链技术的分析和思考[EB/OL]. http://blog.sina.com.cn/s/blog_12f0cb2060102z7iq.html.
[39] Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments, 2016.
[40] WeCross 技术文档[EB/OL]. https://fintech.webank.com/developer/docs/wecross/.
[41] Web-Based XCAT tool for easy ZEC/BTC atomic trading.[EB/OL]. https://github.com/ZcashFoundation/GrantProposals-2017Q4/issues/29.
[42] Yu G, Wang X, Yu K, et al. Survey: Sharding in blockchains[J]. IEEE Access, 2020, 8: 14155-14181.
[43] Kokoris-Kogias E, Jovanovic P, Gasser L, et al. Omniledger: A secure, scale-out, decentralized ledger via sharding[C]. 2018 IEEE Symposium on Security and Privacy (SP), 2018: 583-598.
[44] Elrond A Highly Scalable Public Blockchain via Adaptive State Sharding and Secure Proof of Stake[EB/OL]. https://elrond.com/assets/files/elrond-whitepaper.pdf.
[45] Eykholt E, Meredith L G, Denman J. RChain Architecture Documentation[J], 2017.

[46] EKT Whitepaper[EB/OL]. https://github.com/shangsony/EKT/blob/master/docs/whitepaper.md.
[47] FUSION Whitepaper: An Inclusive Cryptofinance Platform Based on Blockchain[EB/OL]. https://uploads-ssl.webflow.com/5cbf7269aa4c8ec895500d90/5cd19865da79bd05684babfc_Fusion%20White%20Paper.pdf.
[48] Building Super Financial Markets for the New Digital Economy[EB/OL]. https://www.wanchain.org/files/Wanchain-Whitepaper-EN-version.pdf.
[49] NULS WHITEPAPER 2.0[EB/OL]. https://www.nuls.io/wp-content/uploads/2019/06/NULS_Whitepaper_2.0.pdf.
[50] Chainlink's Documentation[EB/OL]. https://docs.chain.link/docs.
[51] Snow P, Deery B, Lu J, et al. Factom: Business processes secured by immutable audit trails on the blockchain[J]. Whitepaper, Factom, November, 2014.
[52] PalletOne [EB/OL]. http://pallet.one/.
[53] Huang H, Kong W, Zhou S, et al. A Survey of State-of-the-Art on Blockchains: Theories, Modelings, and Tools[J], 2020.
[54] Spoke M, Team N. Aion: Enabling the decentralized internet[J]. AION, White Paper, Jul, 2017.
[55] Mimblewimble[EB/OL]. https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf.
[56] 火币区块链产业专题报告[EB/OL]. https://www.jianshu.com/p/f2d2e83473fc.
[57] 李燕, 马海英, 王占君. 区块链关键技术的研究进展[J]. 计算机工程与应用, 2019, (20).
[58] Ding D, Duan T, Jia L, et al. InterChain: A Framework to Support Blockchain Interoperability[J].
[59] Privacy on the Blockchain[EB/OL]. https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/.
[60] 怎么在区块链上保护隐私[EB/OL]. https://blog.csdn.net/shangsongwww/article/details/90112431.
[61] 李旭东, 牛玉坤, 魏凌波, et al. 比特币隐私保护综述[J]. 密码学报, 2019, 006(2): 133-149.
[62] Hosp D, Hoenisch T, Kittiwongsunthorn P. COMIT-Cryptographically-secure Off-chain Multi-asset Instant Transaction Network[J]. arXiv preprint arXiv:1810.02174, 2018.
[63] BOSCORE, DPoS Batch PBFT, EOS Consensus upgrade[EB/OL]. https://medium.com/boscore/boscore-dpos-batch-pbft-eos-consensus-upgrade-ff53a2e08b16.
[64] Zhao Guo S G, Shengli Zhang,Lingyang Song,Hui Wang. Analysis of cross-chain technology of blockchain[J]. Chinese Journal on Internet of Things, 2020, 4(2): 35-48.
[65] Herlihy M. Atomic Cross-Chain Swaps[J], 2018.
[66] Sen-Peng T, Chao Y. Research and Improvement of Blockchain's DPoS Consensus Mechanism[J]. Modern Computer, 2019.

[67] Wang J, Wang H. Monoxide: Scale out blockchains with asynchronous consensus zones[C]. 16th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 19), 2019: 95-112.
[68] Zamani M, Movahedi M, Raykova M. RapidChain: Scaling Blockchain via Full Sharding[C]. the 2018 ACM SIGSAC Conference, 2018.