计算机科学与探索
Journal of Frontiers of Computer Science and Technology doi: 10.3778/j.issn.1673-9418.2212081

区块链互操作性及跨链技术研究

王群[1,2]，李馥娟[1,3+]，倪雪莉[1,2]，夏玲玲[1,2]，梁广俊[1,2]，马卓[1,2]

1. 江苏警官学院 计算机信息与网络安全系，南京 210031
2. 江苏省电子数据取证分析工程研究中心，南京 210031
3. 计算机软件新技术国家重点实验室(南京大学)，南京 210093
+ 通信作者 E-mail: lfj@jspi.edu.cn

摘 要:区块链是一项多方共识、可溯源、防篡改的分布式账本技术，为构建高效、可信、安全的数据共享机制和优化业务流程提供了广阔的应用前景。然而，当区块链正处于百花齐放的快速发展阶段时，如何实现信息的跨链交互和价值的跨链转移，成为区块链向纵深伸延过程中亟待解决的问题。首先，在综述已有研究成果的基础上，提出了区块链互操作性的概念，并将其分为链间互操作、层间互操作、分叉间互操作、片间互操作和链上链下互操作 5 个方面进行了讨论；其次，通过梳理区块链跨链操作的演进和实现方式，并借鉴 TCP/IP 体系结构，设计了跨链操作模型，对主要实现步骤进行了功能描述；再次，针对当前区块链跨链操作研究现状，选择了公证人机制、侧链/中继、哈希锁定和分布式私钥控制 4 类区块链跨链操作关键技术进行了重点分析；然后，结合技术特点和应用场景，突出应用示范，选取了部分典型跨链应用项目进行了介绍，并对区块链跨链操作的安全性进行了分析；最后，总结探索了区块链互操作性和跨链技术的未来发展趋势。

关键词: 区块链;互操作性; 跨链技术;信息交换; 价值转移

文献标志码：A **中图分类号**：TP309.7

Research on Blockchain Interoperability and Cross-chain Technology

WANG Qun[1,2], LI Fujuan[1,3+], NI Xueli[1,2], XIA Lingling[1,2], LIANG Guangjun[1,2], MA Zhuo[1,2]

1. Department of Computer Information and Cybersecurity，Jiangsu Police Institute,Nanjing 210031, China
2. Jiangsu Electronic Data Forensics and Analysis Engineering Research Center, Nanjing 210031, China
3. State Key Lab. for Novel Software Technology,Nanjing University, Nanjing 210093, China

Abstract: Blockchain is a distributed ledger technology with multi-party consensus, traceability and tamper-proof, which provides a broad application prospect for constructing efficient, trusted and secure data sharing mechanism and optimizing business processes. However, when blockchain is in the rapid development stage of a hundred flowers blossoming, how to realize cross-chain interaction of information and cross-chain transfer of value has become an urgent problem to be solved in the process of blockchain extension to depth. Firstly, based on the review of the existing research results, the concept of blockchain interoperability was proposed, and it was divided into five aspects: inter-chain interoperability, inter-layer interoperability, inter-fork interoperability, inter-slice interoperability

基金项目：国家自然科学基金（62272203）；江苏省高校自然科学研究重大项目（20KJA520004）；江苏省高校优秀科技创新团队；公安技术、网络空间安全“十四五”江苏省重点学科；计算机软件新技术国家重点实验室（南京大学）开放课题（KFKT2022B23）。

This work was supported by the National Natural Science Foundation of China (62272203), the Natural Science Research Major Project of Jiangsu Provincial (20KJA520004) and the Excellent Scientific and Technological Innovation Team of Jiangsu Universities, Key disciplines of Jiangsu Province in the 14th Five-Year Plan:Public Security Technology and Cyberspace Security，State Key Lab. for Novel Software Technology (Nanjing University)(KFKT2022B23).

and interoperability between on-chain and off-chain. Secondly, by sorting out the evolution and implementation of cross-chain operation of blockchain, and referring to the TCP/IP architecture, a cross-chain operation model was designed, and the main implementation steps were functionally described. Thirdly, in view of the current research status of cross-chain operation, four key technologies of cross-chain operation, including notary mechanism, side chain/relay, hash lock and distributed private key control, were selected for analysis. Then, combined with the technical characteristics and application scenarios, the application demonstration was highlighted, some typical cross-chain application projects were introduced, and the security of blockchain cross-chain operation was analyzed. Finally, the future development trend of blockchain interoperability and cross-chain technology was summarized and explored.

Key words: blockchain; interoperability; cross-chain; information exchange; value transfer

区块链在有效推动了信息网络向着价值网络转变的同时，同样面临着类似传统信息网络经历的从独立到统一、从相互隔离到互联互通的挑战。1961 年 5 月，MIT（Massachusetts Institute of Technology，麻省理工学院）的 Leonard Kleinrock 发表了名为“Information Flow in Large Communication Nets”的论文，首次提出分组交换（packet switching，PS）的概念，为现代互联网技术的发展奠定了基础。1969 年 11 月，基于分组交换技术的全球第一个计算机网络 ARPAnet 问世，拉开了现代计算机网络发展的大幕。不过，在之后较长一段时间内，使用不同协议和组网技术的计算机网络（局域网）之间各自为阵，相互之间无法直接进行连接。直至 1983 年 1 月，ARPAnet 由 TCP/IP 协议取代了原来使用的 NCP（network control protocol，网络控制协议），计算机网络才真正打破隔离，走向融合，真正意义上的互联网开始出现。脱胎于比特币系统的区块链技术，自 2008 年问世以来，在共识机制、区块结构、可编程语言、密码学算法等方面得到了快速发展，产生了大量创新性应用。然而，大量功能各异、性能不同的区块链项目在打破传统集中式管理模式和理念的同时，独立、封闭、单一的运行现状已成为阻碍区块链向着纵深发展的主要阻力，开放、互联、共享的理念成为区块链发展的趋势和选择。

区块链通过分布式账本、P2P 网络、去中心化共识算法、可编程脚本以及必要的经济激励机制等要素，在一个没有第三方可信机构干预的互不信任的节点之间共同维护一个采用密码学方式链接的有序增长的区块列表，实现了价值与信息的同步传输与转移[1]。比特币（Bitcoin 或 BTC）系统不但为区块链应用奠定了难以撼动的基础，而且成为区块链技术最具代表性和最具影响力的应用场景。以太坊（Ethereum 或 ETH）等开源项目以及大量去中心化应用（decentralized application，DApp）的落地，使区块链技术不但为构建数字货币体系提供了坚实保障，而且在金融领域（跨境支付、保险、数字票据、银行征信等）、医疗、物联网、数字版权与文化娱乐、公共服务与教育、社会管理（物资流转、疫情预警、舆情监控等）等领域得到了快速发展，“区块链+金融”、“区块链+医疗”、“区块链+政务”等新型业态出现并得到关注。与此同时，传统计算机网络发展中曾经遇到的互联互通问题在区块链应用中似乎在重蹈着某种历史规律一样同样出现，跨链技术作为目前解决区块链数据孤岛问题，实现资产及功能状态的互相传递、转移和交换，倍受研究者的关注。

早期的计算机组网技术主要由各计算机设备制造商针对自己制造的计算机来设计开发，而未考虑兼容不同品牌的计算机。这一现象同样出现在区块链中，区块链技术起源于比特币，而比特币的设计初衷是通过去中心化方式在开放网络环境中构建一个点对点的电子现金系统，主要针对的是加密数字货币的交易信息，强调了防篡改、可溯源、防止双重支付等金融功能的实现，而忽视了向数字货币之外的其他领域的扩展，从而在安全性、可扩展性、图灵完备等方面存在着不足，不仅影响着比特币自身的发展，而且限制了区块链技术向其他领域的有效扩展。在此背景下，研究者在对比特币系统进行不断优化完善的同时，根据不同应用场景的需求，相继开发了各类独立运行的区块链项目。功能各异的区块链项目在丰富了应用的同时，系统运行

的封闭性导致数据和价值只能在单一区块链内部或极其有限的区块链之间流通，链与链之间缺乏人们期待中的关联性。如何打破现存的“数据和价值孤岛”，实现链与链之间的互联互通，成为当前区块链应用亟待解决的重大问题，跨链技术是解决这一问题的有效手段。

随着区块链项目的不断丰富，人们对区块链间的信息和价值流通需求越来越迫切，也促使国内外研究者聚焦于对该领域的理论研究和实践探索。本文在广泛收集和分析国内外相关文献资料以及对区块链应用现状及发展趋势进行深入分析的基础上，讨论了区块链的互操作性，梳理了跨链技术产生的动因以及发展历程，提出了跨链操作的基本模型和概念，分析了典型跨链技术及项目，并重点从跨链技术自身和跨链操作过程两个方面探讨了跨链操作面临的安全问题，文章最后总结了跨链技术的发展和研究趋势。

1 区块链的互操作性

今天的互联网其实质是一个借助相应的可路由协议（如 RIP、OSPF、BGP 等）使分布在不同地理位置的异构局域网之间实现互连互通的泛在互联接网络，互操作性（Interoperability）是实现互联互通的前提，也是需要重点解决的关键技术。未来的区块链网络发展，同样也要走与今天互联网类似的道路[2-3]。

1.1 区块链互操作性概念

IEEE（Institute of Electrical and Electronics Engineers，电气与电子工程师协会）对互操作性的定义是：在两个或多个系统之间进行信息交换，以及对交换后的信息进一步利用的能力[4]；百度百科对互操作性的定义是：互操作性又称互用性，是指不同的计算机系统、网络、操作系统和应用程序一起工作并共享信息的能力。分析发现，不同的研究人员基于各自的研究背景和行业应用特点，对区块链互操作性存在不同的理解，并从不同层次提出了相应的解决方案和思路。从网络体系的视角，互操作性同时涉及语法互操作性和语义互操作性；从信息交换共享和交换的角度，针对区块链的互操作同时涉及数据共享、统一身份认证、共识算法之间的相互转换和治理过程的协同等要求。本文将互操作性概述为不同实体之间信息交互与共享以及相互之间的协同能力。这里的实体既可以位于同一节点的不同层，也可以分属于不同的节点中。

目前，业界对区块链互操作形成广义和狭义两种认识。其中，文献[5]认为广义的区块链互操作包括链间互操作、层间互操作和链上链下互操作 3 种类型，本文认为广义的区块链互操作在文献[5]的基础上，还应该包括区块链发生分叉后的“分叉间互操作”和区块链进行分片后的“片间互操作”2 种类型，工作示意图如图 1 所示。狭义的区块链互操作特指区块链之间的跨链操作。广义的认识更加全面，而狭义的认识更加具体和有针对性。

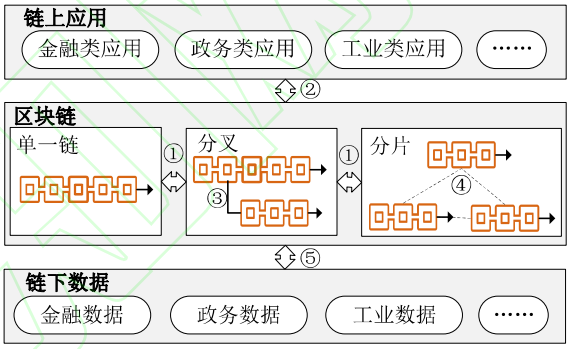

Fig.1 Schematic diagram of generalized blockchain interoperability

图 1 广义区块链互操作示意图

1.2 区块链互操作的分类及实现

根据图 1 所示，对区块链互操作主要涉及到的 5 个方面进行讨论。

（1）链间互操作。链间互操作即跨链操作，具体指在两个或多个区块链之间通过协商确定的接口、通信协议、共识机制实现信息交换和价值转移的能力。链间互操作通过构建链与链之间可靠通道的跨链技术来实现，不同的跨链技术同时遵循体现语法互操作性和语义互操作性的跨链协议。作为区块链应用向外延伸的桥梁，在公有链环境中，跨链操作主要针对各类加密数字货币应用场景，解决不同币种在链间的自由流动，以实现跨平台支付等功能；针对联盟链应用，跨链操作主要面向不同的行业应用，打破联盟间固守的壁垒，实现链与链之间的互联互通。

（2）层间互操作。层间互操作主要解决链上应用（各类 App）与底层区块链之间的信息交互问题，以发挥底层区块链的身份认证、交易发送、合约部署、信息查询等服务能力。层间互操作通过位于上下层之间的接口实现，位于底层的区块链通过

接口向应用层提供所需要的服务，位于上层的不同应用通过接口调用所需要的区块链服务功能。为尽可能提升底层区块链的服务能力，为上层应用提供所需要的安全性和可扩展性，并降低开发者的技术门槛，区块链平台需要为开发者提供所需要的各类功能接口，如合约接口、交易接口、区块接口、系统管理接口等。

（3）分叉间互操作。分叉（fork）是区块链系统在运行过程中因共识机制或协议规则的改变导致的在原来单一主链上派生出另一条支链的现象。其中，基于相同共识机制产生的分叉通常为临时性分叉，其中比特币系统利用“最大工作量原则”解决临时分叉问题[6]，而以太坊系统利用 GHOST（Greedy Heaviest Observed Subtree）协议处理临时分叉[7]。因修改底层协议规则后产生的分叉一般为永久性分叉，将出现同时运行在不同共识机制下的新旧两条链。无论是临时性分叉还是永久性分叉，每条分叉都代表一条独立的链，链与链之间需要进行信息的交互。临时性分叉产生后，需要通过链间信息交互，去掉临时出现的“孤块”，使系统重新收敛到一致状态。对于发生的永久性分叉，不同分叉之间的操作属于同构链间的互操作现象。

（4）片间互操作。分片（sharding）是通过对区块链进行扩容从而提高交易吞吐量、降低交易延迟、提升可扩展性的一种方案[8]。根据实现方式的不同，区块链分片主要有网络分片、交易分片、状态分片等类型。以网络分片为例，通过分片技术将整个区块链网络根据业务需要划分成多个子网络，位于不同子网络中的节点之间负责处理本网络内部的事务，并保存本网络的状态。这里的每个子网络称为一个分片。不同的分片独立处理事务，以提升区块链整体的吞吐量和效率。区块链分片后，同一分片内部的节点之间以及不同分片之间都需要进行信息交换，片间互操作描述的便是分片后的信息交换能力。网络分片后，在进行跨分片交易时，不同分片之间需要进行协调，才能完成分片操作。例如，在同步方式下，通过位于不同分片中的验证节点之间的协作来完成分片交易。而在异步方式下，因为跨分片交易需要在不同的分片中异步执行，所以发送方所在分片必须与接收方所在分片之间进行信息互换，才能确保其任务的完成。另外，在以太坊从 PoW（proof of work，工作量证明）向 PoS（proof of stock，权益证明）升级后，原有链将转变为 1 条主链（main chain）和 100 个分片链（shard chain），其中交易信息、账户信息和合约信息保存在分片链上。作为互连分片链的主链，除要求维护验证节点的状态外，还需要跟踪分片链的运行状态[9]。每个分片链之间以及分片链与主链之间需要交互信息，以确保整个系统的有序运行。还有，在区块链向着连接物理世界和网络空间的物联网（Internet of Things，IoT）延伸过程中，安全和效率成为两个亟待解决的问题。为此，文献[10]提出了一种基于声誉驱动的动态节点安全分片共识模型(reputation-driven dynamic node security sharding consensus model，RDSCM)，该模型通过不同的节点配置，一方面降低了异常节点成为主节点的概率，另一方面保证了分片的可靠性，提高了区块链的吞吐量。

（5）链上链下互操作。链上链下互操作是指区块链系统与链下业务系统之间进行信息交互的能力。链上链下互操作在发挥区块链去中心化应用功能的同时，有效扩展了区块链的数据来源，并实现了链上链下数据交换的安全性、可信性和合规性。一方面，为确保线上业务的正常运行，需要可靠、安全的线下数据的支撑。另一方面，为使区块链支持计算密集型的应用，大量数据的处理需要在线下完成后再将结果提交给线上业务系统。在链上链下互操作中，需要从数据来源、计算和传输等环节确保数据的可信性，需要借助数据加密、通道加密、可信计算、数据脱敏等手段对数据隐私进行保护，另外还需要加强对数据交换的安全监管和审计[11]。

为便于对不同类型互操作的理解和研究，表 2 从实现范围（所采用的区块链底层技术）、研究重点和应用场景 3 个方面进行了对比分析。

Table 1 Comparative analysis of different types of interoperation

表 1 不同类型互操作之间的比较分析

互操作类型	实现范围	研究重点	应用场景
链间互操作	异构链之间	接入规则、通信协议、数据的可靠	解决不同区块链之间的交互

		性、跨链协同等	
层间互操作	同构或异构链之间	接口标准研制、用户和节点管理等	解决上层应用与底层区块链之间的交互
分叉互操作	同构链（原始链与分叉链）之间	共识转换、防止恶意节点作恶等	解决原始链与分叉链之间的交互
片间互操作	同构链（主链与分片链以及不同分片链）之间	分片链与主链间的协同、数据库管理技术、共识转换等	解决主链与分片链以及不同分片链之间的交互
链上链下互操作	区块链与链下系统之间	数据的可信性与安全性、隐私保护、计算安全、安全监管等	解决区块链系统与链下业务系统之间的交互

本文在明晰了区块链互操作边界范围和主要对象的基础上，认为跨链操作是解决区块链互操作性以及实现链与链之间有效互联的核心和关键。为此，本文以跨链操作为重点，同时结合其他的互操作机制，讨论区块链之间的价值转移和信息交互技术。

2 跨链操作概述

2.1 跨链操作的产生与发展

像传统互联网一样，区块链的跨链需求也是随着应用发展，从解决单一问题向着实现复杂环境下的操作要求而产生的。

2012 年，Ripple（瑞波）实验室提出了 InterLedger 协议[12]，该协议力求建立一套能够包容不同账本之间差异性的通用区块链协议，用于解决不同区块链系统之间的相互协作问题。

2013 年 5 月，Thomas Nolan 基于比特币系统提出了区块链原子转移（atomic transfers）[13]方法，其方法基于哈希锁定（hashlock）技术，在比特币系统及其他数字货币区块链系统上通过设置脚本，将获知某个哈希值的原像（preimage）作为触发该脚本运行的条件，从而实现跨链操作的原子性。原子转移也称为原子交换（atomic swap）或原子跨链交换（atomic cross-chain swap）[14]，是指操作参与方必须按约定同步进行，任何一方不能违背协议规定。原子交换在没有第三方参与的情况下，为不同类型区块链资产的点对点转移提供了协议支撑和技术保障。

2014 年 10 月，Adam Back 等人[15]提出了楔入式侧链（pegged sidechains）的概念，用于实现比特币以及其他数字货币之间区块链资产的跨链转移，同时允许用户在比特币系统基础上通过侧链技术开发新的加密数字货币系统，并实现与比特币系统之间的相互操作。对于主链来说，虽然主、侧链之间可以进行资产的相互转移操作，但侧链具有独立性，当侧链受到安全威胁时不会影响到主链的正常运行。侧链技术已经发现成为目前主流的跨链技术。侧链技术的基础是双向楔入（two-way peg），它定义了一种在不同区块链之间进行资产转移的交换机制，可进一步分为对称式双向楔入（symmetric two-way peg）和非对称式双向楔入（asymmetric two-way peg）两种方式，其中，前一种方式从主链到侧链以及反向的传输机制是相同的，后一种方式中主链不知道侧链的状态，而侧链能够知道主侧的状态并完成从主链接收到的数据的验证。

2015 年 2 月，Joseph Poon 等人[16]在发布的闪电网络（lightning network）白皮书中基于比特币系统提出了链下交易技术，该技术使交易通过微支付通道（micropayment channels）网络发送，价值在区块链外（链下）进行转移。作为一种发生在区块链内部的跨链操作机制，链下交易技术在较大程度上提高了交易的效率。2017 年 11 月，基于闪电网络的链下交易技术，首次实现了比特币与莱特币（Litecoin 或 LTC）之间的跨链原子交易。闪电网络的核心包括 HTLC（hashed timelock contract，哈希时间锁定合约）、RSMC（recoverable sequence maturity contract，序列到期可撤销合约）和支付通道。

2016 年 5 月，美国以太坊区块链软件公司 ConsenSys 开发了 BTC Relay[17]，允许用户直接通过以太坊访问比特币系统，即实现 ETH 与 BTC 之间的跨链操作。BTC Relay 技术的实现综合了 BTC 区块头信息与 ETH 智能合约功能，其实质是运行于以太坊的智能合约在不需要第三方中介参与的情况下能够安全的验证 BTC 交易。

2016 年 6 月，Jae Kwon 等人[18]提出了支持不同类型区块链网络接入与实现互操作的区块链网络架构 Cosmos，其初衷是建立一个区块链互联网

络。Cosmos 借鉴了传统互联网集线器（hub）和分区（zones）的概念，其中在分区中运行经典的拜占庭容错（byzantine fault tolerance，BFT）算法 Tendermint，分区在接入不同的区块链后，由集线器负责不同分区之间的通信，集线器遵循 IBC（inter blockchain communication，链间通信）协议。

2016 年 11 月，Gavin Wood 在 Polkadot 白皮书[19]中介绍了一种异构多链体系结构，主要由中继链、平行链和转接桥组成，其目的是实现现有区块链系统及发展中的去中心化 Web3.0 之间的互连互通，其中，中继链负责各个独立区块链网络的接入并实现不同区块链间的信息交换和无需建立信任环境下的交易。同时，Polkadot 作为一个通信协议，与传统互联网中的 TCP/IP 协议一样，实现了不同区块链之间信息的相互交换，但作为一种链间通信协议，Polkadot 还会对消息的有效性和到达顺序进行验证。

在 2016 年 11 月发布的以太坊分片（sharding）[20]技术文档中，在以太坊共识机制从 PoW（proof of stock，工作量证明）过渡到 PoS（proof of stake，权益证明）后，以太坊的网络结构将由主链（main chain）和分片链（shard chain）组成，用户的交易信息存储在主链上，分片链主要处理交易和存储账户与合约状态，每个分片链与主链之间进行信息交换。分片是一种链上解决方案，它通过优化主链自身的协议来改善其性能。

2017 年 1 月，Ede Eykholt 等人在发布的《RChain Architecture Documentation》[21]技术文档中提出了一个可并发、可重组、可伸缩的能够为企业提供高性能服务的区块链服务平台 Rchain，该平台源于一种基于形式化验证、去中心化的并行计算模型，融合了分片技术、Casper 协议、形式化验证、高并发 RhLang 语言、RhoVM 虚拟机等创新技术，主要解决区块链底层协议的扩展、智能合约的形式化验证、共识机制的安全及经济激励等问题。Rchain 通过定义类似传统互联网的命名空间（namespace），在每个命名空间中运行有一个独立的区块链网络，不同命名空间可以相互通信。

2017 年 2 月，Block Collider（后更名为 Overline）项目[22]通过将不同的区块链整合从而构建了一个跨多个区块链的高速分布式账本，其中，通过 FIX（financial information eXchange，金融信息交换）协议，将各类区块链数据头部结构进行整合和统一，使不同区块链系统都能够进行识别和交换，以提高多链操作的速度和吞吐量；Overline 通过优化 Bitcoin 的“中本聪共识”(nakamoto consensus)，使用了 PoD（proof of distance，距离证明）共识机制，从而提高了区块链之间的互操作性。

2017 年 7 月，Matthew Spoke 和 Nuco Engineering Team 提出了 Aion 协议[23]，为不同区块链系统的互连提供通用的通信协议和规范（类似于 TCP/IP 协议栈）。Aion 网络的核心是一个专门设计的、公开的第三代区块链，用于连接大量区块链并管理链上的应用程序，同时为不同区块链之间的互操作提供了相应的经济激励机制。基于 Aion 网络，可以实现任何与 Aion 兼容的区块链和以太坊之间的数据交换，并提供了较强的数据处理能力和较大的存储容量，同时，允许基于不同的共识机制创建所需要的公有链或私有链。

2017 年 8 月，Joseph Poon（闪电网络创始人）和 Vitalik Buterin（ETH 创始人）共同提出了可伸缩的智能合约 Plasma[24]，其实质是一套为各种不同区块链项目提供链下解决方案的框架，该架构采取树形结构，树根代表主链，树的各个分支代表独立的区块链，以此来实现区块链的扩容；2018 年 1 月，Vitalik Buterin 提出了 MVP（minimal viable Plasma，最小可行 Plasma）[25]，旨在采用一种简单的方式提供 Plasma 的基本安全特性；2018 年 1 月，Vitalik Buterin 在 Plasma 基础上又提出了 Plasma Cash[26]，对 Plasma 进行了部分实现功能的改进，其中，使用稀疏 Merkle 树代替了标准 Merkle 树来存储和转移非同质（non fungible）代币等；为了解决 plasma cash 中代币的不可分割性导致的无法进行小额交易问题，2018 年 6 月，Dan Robinson 提出了 Plasma Debit[27]，在性能、可用性等方面进行了优化；另外，针对 MVP 中当用户离开网络时需要确认签名（confirmation signature）带来的不便，2018 年 6 月，Ben Jones 和 Kelvin Fichter 提出了 More VP(More Viable Plasma)[28]，移除了确认签名的要求。需要说明的是，由于 Plasma 在跨链技术中的重要性，研究人员在 Plasma 框架基础上提出了大量改进版本，不断对其进行发展完善。

2018 年 5 月，一种基于 Omni Layer 协议（该协议运行 Bitcoin 区块链上）、在 Bitcoin Cash（BCH）区块链上实现智能合约的协议规范 Wormhole[29]推出，其中使用的基础货币为 WHC（Wormhole Cash）。Wormhole 在不改变现有 Bitcoin Cash 共识机制的前提下，通过桥接方式实现了与其他类型区块链之间的互联和资产交换。Wormhole 刚刚推出时就同时支持 Terra、Solana、Ethereum、Binance Smart Chain、Avalanche 和 Polygon 之间的互联。Wormhole 的发展分为 Earth(地球)、Tropos(对流)、Ionize(电离)和 Exophere(外逸)4 个阶段，从实现 Wormhole 协议从 Omni Layer 协议分离，到最后的任何开发者都可以发布智能合约到网络中运行。

2019 年 8 月，Li Dawei 等人提出了一种基于多重签名的跨链系统 AgentChain[30]，该系统为交易操作者提供了一个开放平台，通过锁定代币来将交易操作者划分为多个去中心化的交易组，用户可以选择一个信誉良好的交易组，并将资产存入现有区块链上经多重签名的交易组地址。然后，资产将被交易组映射到 AgentChain，交易组支持以代币形式的交易。AgentChain 与大多数现有的区块链项目兼容，只要区块链系统支持多重签名即可。

2020 年 8 月，Aleksei Pupyshev 等人提出了一种区块链不可知（blockchain-agnostic）的跨链通信和数据预言机协议 Gravity[31]，该协议通过创建网关、跨链应用程序和侧链等机制实现跨链操作，同时，充分利用了各自治系统原有的稳定性和安全性，而且回避了对公共区块链及代币的依赖。

2021 年 1 月，Rongjian Lan 等人提出了一种基于智能合约执行的用于将资产从一个拜占庭容错区块链系统转移到另一个区块链系统(如以太坊)的跨链网桥协议 Horizon[32]，作为一种跨链桥接协议，该协议允许在链上交换加密货币，在链上将资产转移到侧链，以及在不同分片中对事务进行跨分片验证，同时实现了 BFT 区块链与其他区块链之间的互操作。

2022 年 1 月，Martin Westerkamp 和 Maximilian Diez 共同提出了第一个链中继方案 Verilay[33]，该方案不需要修改原区块链协议或验证器，区块提议者的签名通过目标区块链上的一个专用中继智能合约进行验证，可以验证产生最终区块的 PoS 协议（如以太坊 2.0、Cosmos、Polkadot 等）。与 PoW 链中继相比，Verilay 只需要提交区块头部信息就可以完成验证操作，提高了系统的可伸缩性。

2022 年 5 月，Hei 等人提出一个称为 Practical AgentChain[34] 的跨链交换系统，通过采取优化的共识算法、智能合约和交换协议，实现了不同代币之间的跨链交易。

近年来，随着跨链操作需求越来越急迫，针对跨链技术的研究已成为区块链领域研究的一个重点、热点和难点。表 2 重点从适用场景和实现机制 2 个方面对比了跨链操作发展历程中的典型技术和应用，其中，在适用场景中，除典型的 BTC 和 ETH 外，其他都归为自建区块链（包括公有链、联盟链和私有链）；实现机制主要包括通信协议、哈希锁定、侧链、中继、分片、硬分叉等。

Table 2　Development history of cross-chain operation

表 2　跨链操作发展历程

名称	年份	适用场景	实现机制
InterLedger[12]	2012	自建区块链	通信协议
atomic transfers[13]	2013	BTC 及其他数字货币	哈希锁定
pegged sidechains[15]	2014	BTC 及其他数字货币	侧链
lightning network[16]	2015	BTC	哈希锁定
BTC Relay[17]	2016	ETH	侧链
Cosmos[18]	2016	自建区块链	通信协议
Polkadot[19]	2016	自建区块链	中继
Sharding[20]	2016	ETH	分片
Rchain[21]	2017	自建区块链	通信协议
Overline[22]	2017	自建区块链	通信协议
Aion[23]	2017	自建区块链	通信协议
Plasma[24]	2017	ETH	侧链
MVP[25]	2018	ETH	侧链
Plasma Cash[26]	2018	ETH	侧链
Plasma Debit[27]	2018	ETH	侧链
More VP[28]	2018	ETH	侧链
Wormhole[29]	2018	BCH 及其他数字货币	桥接
AgentChain[30]	2019	已有和自建区块链	代理
Gravity[31]	2020	已有和自建区块链	通信协议
Horizon[32]	2021	BFT 与其他区块链	桥接
Verilay[33]	2022	基于 PoS 的区块链	中继
Practical AgentChain[34]	2022	已有和自建区块链	通信协议

2.2 跨链操作模型

借鉴 TCP/IP 体系结构，针对区块链技术和应用特点，本文提出如图 2 所示的跨链操作模型，按其操作过程，主要分为 4 个步骤。

（1）接入网络。区块链系统通过接入网络加

入链联网，实现与其他区块链系统之间的信息交换。出于安全考虑和管理需要，区块链以跨链方式接入链联网时需要有相应的接入机制作为保障。由于联盟链之间一般都提供有明确和相对完善的用户准入机制，而且大量需要进行互联的联盟链之间具有同构性，所以跨链接入方式相对稳定。对于公有链而言，其跨链操作相对复杂，需要同时考虑不同区块链之间在数据结构、接口形式、数据封装格式等方面存在的差异性，需要通过对区块数据结构的抽象，形成统一的标准。目前，区块链跨链接入多采用开放端口、SDK（software development kit，软件开发工具包）和适配器 3 种方式[5]，表 2 所列的跨链操作方案一般都同时支持开放接口和 SDK，其中有部分以及 BitXHub[35]、WeCross[36]等还支持适配器服务，以进一步简化区块链的接入方式。在跨链操作的安全性方面，现有研究中公有链跨链操作一般会采用代币抵押机制，通过经济奖惩手段防止恶意节点可能的作恶行为，维护系统的安全性。

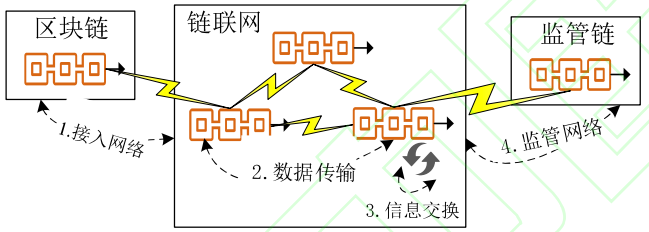

Fig.2 Blockchain cross-chain operation model

图 2 区块链跨链操作模型

（2）数据传输。与组成互联网的局域网不同，区块链是一个相对封装的系统，需要考虑链与链之间以及区块链与链下系统之间的信息交换能力。为了实现跨链操作，尤其是方便、快捷地进行跨链消息的路由与验证，一般需要设计跨链网关来处理跨链消息，然后再利用类似于 TCP/IP 的链间消息传输协议将消息传送到目标区块链。体系结构和通信协议是研究网络的两大核心要素，目前，区块链已形成业界普遍认可且相对稳定的层次模型，但由于不同区块链在其底层数据结构、接口规范、共识机制等核心环节存在较大差异，很难实现不同区块链之间的报文互认和信息共享。在此情况下，需要借鉴 TCP/IP 的成功经验，开发一套实现链与链之间互联的通信协议栈，以屏蔽不同底层区块链在数据结构、报文格式、路由选择、寻址、共识机制等方面存在的差异性，进而实现跨链消息、交易、区块等关键数据在不同链之间的传输、互认和共识。在此领域，已经有一些研究成果，例如 Ripple 的 ILP（InterLedger Protocal）协议、Cosmos 的 IBC 协议、Polkadot 的 XCMP（Cross-Chain Message Passing）协议[37]等，但这些协议或实现方案虽然在一定程度上解决了异构区块链之间的底层互联互通问题，但尚缺乏类似 TCP/IP 的通用标准。

（3）信息交换。当跨链消息到达目标链后，由目标链中相应的节点解析该消息，并执行相应的操作，同时将正确结果或出错信息返回给接入链中对应的节点。在信息交换环节，需要在尽可能简化操作流程和精简控制信息的前提下，重点解决：①消息来源的可信性。消息来源的可信性是跨链操作的基础和前提，BitXHub、Comos、Polkadot 等方案分别通过对交易数据、区块数据、报文结构等数据单位中的相关字段的验证，确保消息的来源是真实可信的；②运行结果的有效性。为了实现运行结果的有效性，需要引入验证机制，对特定字段进行校验；③操作过程的原子性。原子性确保了跨链操作过程的一致性，WeCross、BitXHub 等方案分别采用两阶段提交、哈希时间锁定等机制，再结合过程性消息，实现跨链操作的原子性。

（4）监管网络。类似于 TCP/IP 网络中的 SNMP（simple network management protocol，简单网络管理协议），区块链跨链操作中需要一套通用的管理协议实现对跨链操作的监管，确保跨链操作的安全可靠，实现跨链操作的可持续发展。跨链操作监管的实现路径需要技术和经济奖惩相结合，其中技术方面主要包括跨链身份认证和授权、交易回滚、安全监管、数据安全与隐私保护、系统审计等。相对于联盟链，公有链的监管更为复杂，涉及消息管理、路由选择、共识转换等众多环节。现有的方案也只是初期尝试和探索，大量技术和管理细节还需要随着跨链操作技术的发展和应用推进有针对性的进行研究。

3 跨链技术

跨链操作尚处于发展初期，不同领域的研究者基于不同的研究视角和应用场景提出了一些技术方案。其中，最具代表性的是以太坊创始人 Vitalik Buterin 立足区块链互操作性提出了公证人机制

（notary schemes）、侧链/中继（sidechains/relays）和哈希锁定（hash-locking）3 种跨链技术[38]，David Treat 等人[39]基于 DLT（distributed ledger technology，分布式账本技术）提出跨链操作是通过连接相对独立的区块链系统来实现不同账本之间的可信互操作，WEF（world economic forum，世界经济论坛）聚焦于互操作性的实现路径提出跨链操作的实现包括跨链验证、预言机和 API（application program interface，应用程序接口）网关 3 种方式[40]。另外，通信协议作为网络的核心组成，是各类技术实现的参照和基础，与此同时，随着区块链互操作进程的推进，出现了一些有代表性的跨链操作通信协议。综上分析，本文重点从公证人机制、侧链/中继、哈希锁定、分布式私钥控制和跨链通信协议 5 个方面进行讨论。

3.1 公证人机制

公证人机制是数字货币跨链交易中应用较多且易于实现的一种跨链技术[38]，通过选择产生一个或多个作为共同依赖的公证人，负责监听来自不同链中的请求，在对请求进行验证后，执行该请求事务，然后在目标链执行约定的操作，实现对请求事务的响应。公证人是跨链操作的关键，可由跨链各方共同指定，也可通过密码学技术确定。公证人通过预设的共识算法决定对接收到的请求是否执行，如果执行将达成共识。公证人机制可以分为单签名公证人机制、多重签名公证人机制和分布式多重签名公证人机制 3 种类型。

图 3 以比特币区块链（链 A）中的 Alice 与以太坊区块链（链 B）中的 Bob 通过公证人机制进行数字货币跨链交易为例，分别介绍 3 种公证人机制的实现方法和特点。

（1）单签名公证人机制。单签名公证人机制是一种完全中心化的跨链操作方式，公证人扮演交易确认者和冲突仲裁者的角色，一般由参与跨链的各方共同指定一个第三方可信机构或由共识算法产生的单一节点担任。单签名公证人机制的实现过程为（假设 Alice 用自己的 m 个 BTC 兑换 Bob 的 n 个 ETH（即：m 个 BTC 等价于 n 个 ETH）：

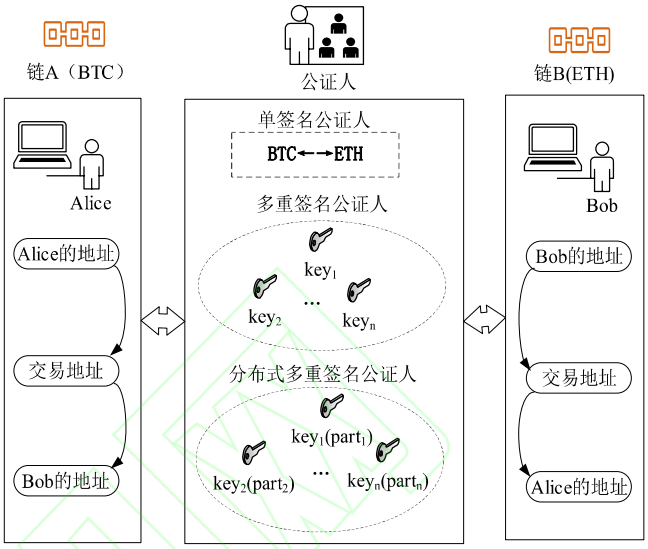

Fig.3 Schematic diagram of the notary schemes

图 3 公证人机制示意图

①链 A 中的 Alice 将自己比特币钱包中的 m 个 BTC 转入公证人指定的交易地址，并告知公证人要与链 B 中的 Bob 进行数字货币的兑换。

②经公证人验证 Alice 消息的合法性后，将该交易请求发送给 Bob。

③在经 Bob 同意后，Bob 将自己钱包中的 n 个 ETH 转入公证人指定的交易地址，公证人验证其合法性。

④公证人将 Alice 的 m 个 BTC 转入 Bob 在链 A 中的地址，将 n 个 ETH 转入 Alice 在链 B 中的地址，至此完成货币的兑换。

由以上操作过程可知，在跨链操作中，公证人担负着信息监听、身份和交易的合法性验证以及交易确认等操作，技术架构简单，适应性强，交易处理速度快，但以中心化模式运行的公证人节点为安全和隐私带来了威胁。

（2）多重签名公证人机制。在单签名公证人机制中，交易的安全性和身份的可靠性高度依赖于公证人的签名，如果公证人被攻击，虚假的签名将会导致跨链操作的错误或失败。多重签名公证人机制利用多重签名技术[41]，由多位公证人同时对交易进行签名，当验证通过后跨链交易才能被确认。在具体实现中，当发生一笔交易时，需要在由 m 个公证人组成的集合中按算法约定选取 n 个公证人（其中，$n \leqslant m$），再利用其私钥 key_1、key_2、……，key_n 共同对交易进行签名，以降低单签名过程对公证人可靠性的依赖性。

（3）分布式多重签名公证人机制。区别于多重签名公证人机制，分布式多重签名公证人机制改进了签名方式：首先，利用密码学技术生成系统中唯一的私钥 k，并将 k 拆分成 $key_1(part_1)$、$key_2(part_2)$、……、$key_n(part_n)$共 n 份；然后，从网络中随机选取 n 个互不信任的节点作为公证人，将拆分后的私钥段分发给每个公证人；最后，由这 n 个公证人共同签名，完成交易的验证和确认。例如，Fusion 区块链利用 DCRM（distributed control rights management，分布式的控制权管理）层来保护链上资产的安全性[42]，通过 DKG（distributed key generation，分布式秘钥产生）技术生成分布式的私钥，通过承诺（commitment）方案实现安全性，通过同态加密技术实现密文处理，通过零知识证明实现验证过程中的隐私保护，最终实现分布式签名算法。

单签名公证人机制、多重签名公证人机制和分布式多重签名公证人机制在密码算法、实现验证、安全性、典型应用等方面的比较如表 3 所示。

Table 3 Comparison of the main performance of different notary schemes

表 3 不同公证人机制的主要性能比较

性能	单一公认人	多重签名	分布式多重签名
加密算法	椭圆曲线加密（ECC）	椭圆曲线加密（ECC）	ECC、DKG、同态加密、零知识证明
中心化程度	中心化	多中心化	去中心化
安全性	较弱	较安全	安全
实现难度	较容易	较复杂	复杂
典型应用	Bitcoin/Ethereum	Bitcoin/Ethereum	FUSION

3.2 侧链/中继

侧链是针对主链而言，是在主链基础上的同构延伸和应用扩展。中继是连接不同链（同构链或异构链）实现价值转移和消息交换的中枢。侧链和中继的技术实现各有侧重，共同用于解决区块链的互联问题。

（1）侧链。侧链特指与主链并行运行的区块链[43]。侧链与主链之间的关系表现为：①针对性。任意一个侧链都是根据特定功能实现需要，针对具体主链而言的；②相对独立性。侧链与主链在运行上相对独立，两者之间是一种松耦合关系，虽然两者属于同构链，但其共识机制可能不同；③互通性。作为一种特殊的跨链方案，侧链技术可以实现价值在主链与侧链之间的按需流通；④可扩展性。通常情况下，侧链是对主链的功能扩展或性能改善，可以根据需要将部分原来在主链上实现的功能或资产转移到侧链上，以达到缓解主链压力和优化主链性能的目的。

侧链方案最早应用在比特币系统中。比特币在创造了区块链应用神话的同时，其先天存在的交易延时长、系统效率低、非图灵完备等缺陷，限制了其功能的扩展。侧链技术通过在主链上创建一条并行运行的新链，实现比特币在主链与侧链之间的等价按需转移，有效解决了比特币系统存在的不足[44]。在比特币系统中，侧链与主链之间数字资产的转移称为双向锚定（two-way peg）[45]，即当资产在主链上被锁定后，等价的资产将会在侧链上释放，同样当等价的资产在侧链中被锁定时，主链中的资产被释放。不论资产位于主链还是侧链，其价值不会发生变化，因为存放在侧链上的资产在主链上都有相应的背书。由于侧链相对独立，所以开发者可以根据应用需要创建适应特定场景应用要求的侧链，同时侧链可以充分利用主链的特性，而不会对主链产生影响。目前，双向锚定仍然是侧链技术的核心。

根据实现模式的不同，双向锚定技术可以分为单一托管、联盟、SPV（simplified payment verification，简单支付验证）、驱动链和混合 5 种模式[44]，其主要性能比较如表 4 所示。

Table 4 Performance comparison of different implementation modes of side chain technology

表 4 侧链技术不同实现模式的性能比较

性能	单一托管	联盟	SPV	驱动链	混合
实现方式	类似单签名公证人机制	类似多重签名公证人机制	对主链进行软分叉	对主链进行软分叉	对主链进行软分叉
实现难度	容易	较容易	较容易	较复杂	复杂
中心化程度	高度中心化	多中心化	去中心化	去中心化	去中心化
实现效率	高	较高	高	较低	低
安全性	弱	较弱	强	强	强

（2）中继。中继即“中间人”，其实质是由被连接的区块链经抽象而形成的一个跨链操作层，是对公证人机制与侧链机制的融合与扩展，其主要功能是作为一个适用于同构链或异构链的通信中枢，在不依赖于任何可信第三方验证的情况下，收集来

自不同区块链（统称为“平行链”）的消息并进行验证和转发[46]。在中继机制中，所有平行链都必须遵守跨链协议规范，实现与中继链的连接[47]。当某一平行链中的节点需要进行跨链操作时，该节点首先发起跨链操作请求，该请求报文将发送到中继链中的验证节点，经验证通过后再由中继链发送到目标平行链，随后在目标平行链上根据共识机制进行公证人的跨链互操作。中继与侧链之间的主要区别如表 5 所示。

Table 5　Main differences between side chain and relay schemes

表 5　侧链与中继机制的主要区别

名称	侧链机制	中继机制
从属关系	侧链从属于主链	链与链之间没有从属关系
主要功能	对主链功能的扩展	跨链数据传输
交易处理	同步区块头数据	不需要同步区块头数据
交易速度	慢	快
安全性	主、侧链独立	链与链之间相依赖

侧链/中继方案基于轻客户端验证技术来实现，验证节点不需要跨链下载完整的账本，只需要执行能够实现轻客户端功能的智能合约，就能够跨链验证某笔交易是否存在。以 SPV 为例，位于 A 链上的验证节点只需要获得 B 链的加密哈希树（cryptographic hash tree）和区块头（block header）[48]，就可能通过智能合约来验证 B 链上某一笔交易是否发生。

3.3 哈希锁定

哈希锁定[49]技术是使用具有哈希锁定机制的合约 HTLC 进行资产锁定，以可编程的形式在去中心化、去信任的环境中以资产质押的形式进行跨链条件支付（conditional payment）[50]。哈希锁定的核心是序贯博弈（sequential game）[51]，即位于同一链或不同链上的用户选择在时间上存在先后顺序的策略，并基于该策略的博弈实现以资产为质押的跨链交易。

哈希锁定的核心是时间锁（time lock）和哈希锁（hash lock）。其中，时间锁是指对于具体的某笔交易，双方约定必须在规定的时间内提交才有效，一旦超时则承诺方案失效。无论是因为交易发起方还是接受方的原因，一旦交易失败，时间锁会让参与方拿回属于自己的资产，避免因欺诈或交易失败带来的损失。哈希锁是指确定一个哈希函数（如 HASH-256），针对对方提供的原像 s，如果得到对应的值 h=hash(s)，则承诺方案有效，否则承诺失效。

从合约实现角度看，HTLC 主要由基于时间锁的时间验证和基于哈希锁的哈希验证组成。下面，分跨链交易和跨链条件支付两种应用类型，分别介绍用户间哈希锁定的实现过程和应用特点。

（1）跨链交易。如图 4 所示，假设位于比特币系统中的 Alice 需要用 m 个 BTC 与位于以太坊系统中 Bob 的 n 个 ETH 进行交换。首先在比特币系统和以太坊系统上部署 HTLC 合约，然后执行以下操作：

①Alice 随机生成一个用于计算哈希函数的原像 s，并计算机其值 h=hash(s)。

②Alice 将 h 发送给 Bob，并调用以太坊系统中的 HTLC 合约。

③Alice 锁定自己的 m 个 BTC，同时设置一个锁定时间 t_1，承诺 Bob：如果在规定的 t_1 时间内能够提供 h 的原像 s，就可以得到 m 个 BTC。

④在 Bob 得知 Alice 锁定了 m 个 BTC 的情况下，也锁定了自己的 n 个 ETH，同时设置了个锁定时间 t_2（$t_2 < t_1$），并承诺 Alice：如果 Alice 在规定的 t_2 时间内能够提供 h 的原像 s，就可以得到 n 个 ETH。

⑤Alice 将 s 发送给 Bob，并调用以太坊中的 HTLC 合约，以获取 n 个 ETH。如果在 t_2 时间内仍未解锁，则 n 个 ETH 返还给 Bob。

⑥Bob 在获得原像 s 后，将其回传给 Alice，通过调用 HTLC 合约以获得 m 个 BTC。如果在 t_1 时间内仍未解锁，系统将返还 m 个 BTC 给 Alice。

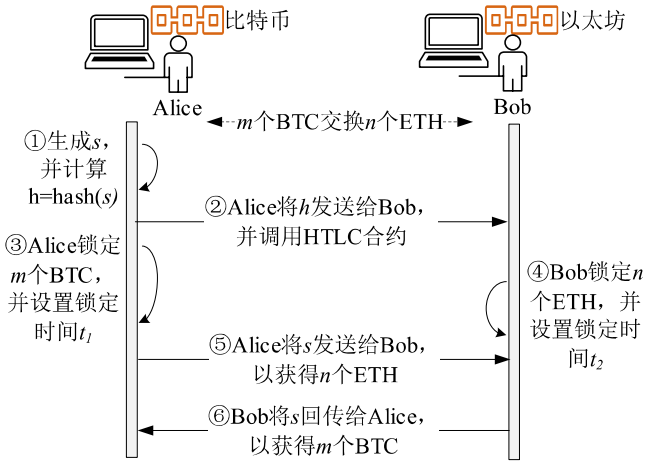

Fig.4 Hashed-locked cross-chain transaction flow

图 4 哈希锁定跨链交易流程

作为价值交换的一种技术，哈希锁定跨链交易的实现需要具备以下条件：①所有涉及到的区块链都要支持相同的哈希算法，如 HASH-256；②所有涉及到的区块链都需要兼容 HTLC 合约，如果是比特币系统其脚本需要兼容 HTLC 合约，如果是以太坊系统其智能合约需要兼容 HTCL 合约；③交易双方都需要在对方的区块链上开设交易账户。

（2）跨链条件支付。多个哈希锁定可以组成多跳支付，交易双方可以借助中间节点来实现跨链操作和原子交换（atomic swap），以满足实际应用场景中的跨链支付需要，如比特币闪电支付网络。如图 5 所示，假设 Alice 需要借助 Trudy 向 Bob 支付 m 个 BTC，具体操作过程为：

①Bob 生成原像 s，并计算哈希值 h=hash(s)，然后将 h 发给 Alice。

②Alice 调用 HTLC 合约向 Trudy 进行条件支付：当且仅当 Trudy 在规定的 t_1 时间内向 Alice 提供哈希值 h 对应的原像 s，Alice 才会向 Trudy 支付 m 个 BTC。同样，Trudy 调用 HTLC 合约向 Bob 进行条件支付：当且仅当 Bob 在规定的 t_2（$t_2 < t_1$）时间内向 Trudy 提供哈希值 h 对应的原像 s，Trudy 才会向 Bob 支付 m 个 BTC。

③Bob 如果能够在 t_2 时间内向 Trudy 提供原像 s，将获得 m 个 BTC，否则 m 个 BTC 将返回给 Trudy，Trudy 不会有任何损失。

④Trudy 如果在 t_1 时间内向 Alice 提供了原像 s，将会获得 m 个 BTC，否则 m 个 BTC 将退还 Alice，Alice 不会遭受任何损失。

通过以上操作流程可以看出，跨链条件支付具有原子性（atomic），即在 HTLC 合约的跨链条件支付过程中，所有参与方的操作要么全部完成，顺利完成支付；要么全不完成，返回质押资产。原像 s 和哈希值 h 即可以在链上传输，也可以在链下传输，然后在链上进行验证，以实现对用户隐私的保护。

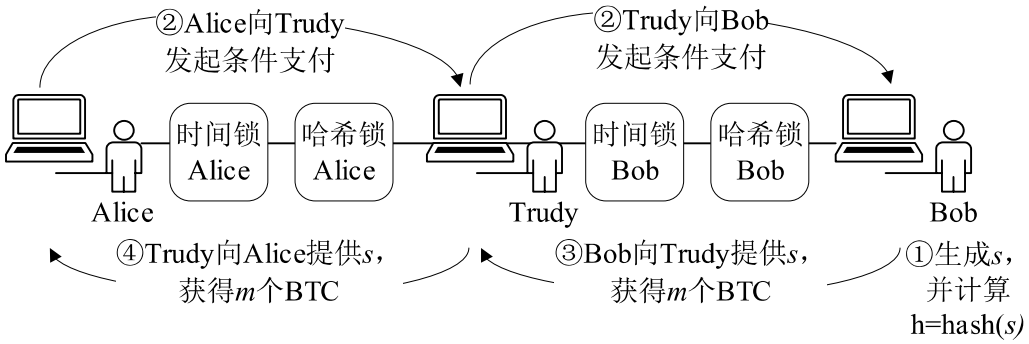

Fig.5 Hashed-locked cross-chain conditional payment flow

图 5 哈希锁定跨链条件支付流程

3.4 分布式私钥控制

在区块链中，用户私钥对应着用户拥有的数字资产。用户之间的资产交换可通过控制用户的私钥来完成。分布式私钥控制（distributed private key control）[52]是基于分布式系统特征，通过分布式节点来控制不同区块链中的各类数字资产对应的私钥，并建立原始链与跨链系统之间的映射关系，从而实现资产在不同区块链之间的转移。分布式私钥控制技术实现了数字资产的所有权与控制权之间的剥离，资产的所有权仍然归用户所有，但控制权转移到去中心化的跨链系统中。

分布式私钥控制中私钥的产生和管理类似于分布式多重签名公证人机制，基于分布式私钥控制机制的跨链操作思路是：存在一个生成密钥对并对私钥进行分布式管理的跨链系统（如 Fusion[42]、Wanchain[53]等），由该系统生成和管理用于不同区块链用户间进行跨链操作的私钥和临时交易地址（公钥），并对交易进行锁定、验证和解锁，完成跨链操作过程。

图 6 仍以 Alice 用 m 个 BTC 与 Bob 的 n 个 ETH 进行交换为例进行说明，具体操作过程为：

①位于比特币原始链中的 Alice 向跨链系统发出跨链操作申请。

②系统生成密钥对（$key_{pub\text{-}Alice}$，$key_{priv\text{-}Alice}$），其中公钥 $key_{pub\text{-}Alice}$ 作为 Alice 在比特币系统中的一个临时交易地址 Add_{Alice}，而私钥 $key_{priv\text{-}Alice}$ 被拆分成 k 份后分发给跨链系统中的每个参与者，每个参考者保存其中的 1 份。

③跨链系统将 Add_{Alice} 发送给 Alice。

④Alice 将 m 个 BTC 存入地址 Add_{Alice}。

⑤跨链系统对 Add_{Alice} 中的交易进行验证，无误后进行锁定。

⑥~⑩的操作流程类似于①~⑤，之后，位于以太坊中的 Bob 将 n 个 ETH 转入临时地址 Add_{Bob}，并进行锁定。

⑪通过分布式私钥管理算法，跨链系统通过密钥管理参与者分别恢复出 Alice 和 Bob 的私钥 $key_{priv\text{-}Alice}$ 和 $key_{priv\text{-}Bob}$，然后将 $key_{priv\text{-}Alice}$ 发给 Bob，将 $key_{priv\text{-}Bob}$ 发给 Alice，这样 Alice 就可以得到 n 个 ETH，而 Bob 将得到 m 个 BTC，实现了跨链交易。

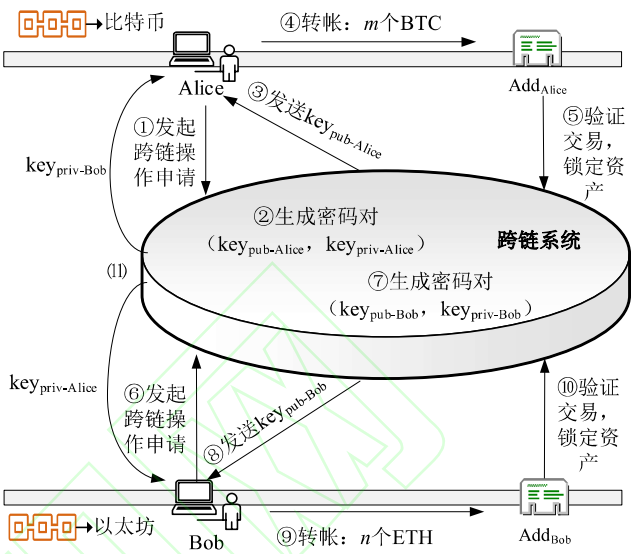

Fig.6 Distributed private key control implementation flow

图 6 分布式私钥控制实现流程

分布式私钥控制机制实现了跨链操作过程中对临时交易账户私钥的分布式管理，避免了中心化风险，而且在不改变原始链的情况下，可以针对不同区块链进行跨链操作，适用性较强。但是，由于各操作过程都依赖于智能合约，所以具有一定的开发难度。

3.5 跨链通信协议

跨链通信协议是指不同区块链系统之间通过相互之间的信息交互和协同，完成信息交换和价值转移必须遵循的规则和约定。具体来讲，需要交流的内容（信息或资产）、手段（智能合约或脚本）及要求（原子性、隐私性等），都必须遵循通信协议这个相互接受的规则。为此，本节立足通信协议的体系特征，综合考虑技术实现、适用范围、安全及隐私、可扩展性等因素，选取几个应用于不同跨链操作场景的典型通信协议簇来分析跨链通信协议的功能及实现方法，而不再拘泥于对单一功能协议的讨论。

（1）IBC 协议。IBC（inter blockchain communication，区块链链间通信）[18,54]协议是一种类似于 TCP 的面向连接的端对端有状态通信协议，用于在不同的分布式账本之间进行可靠和有序的通信，并实现对用户的身份认证。IBC 是针对异构链之间的互操作性特点和需求而设计的，不同区块链系统的分布式账本可能存在于运行在不同通信模型和管理模式的开放网络环境中，而且可能使用不

同的共识算法和底层数据结构。IBC 通过确定协议的数据结构、抽象和语义集来实现具体的功能，并提供了跨链操作的异步通信原语，以便于技术实现。IBC 协议已应用在由 Tendermint 团队构建的开源社区项目 Cosmos 中。IBC 协议在设计上采用了类似 TCP 的概念，一次完整的跨链操作首先需要通过握手过程在不同区块链系统的可信用户之间建立一个可靠的通道（channel）连接，之后基于该通道实现交易的有序转移操作，实现了不同通道之间业务的隔离，提高了通信的安全性和隐私性。

（2）XCMP 协议。XCMP（cross-chain message passing，跨链消息传递）[37,55]是 Polkadot 平台使用的链间消息传输协议，主要用于平行链间传递消息。XCMP 利用 Merkle 树的简单队列机制保证跨链交易的正确性，其中中继链（relay chain）是协议实现的核心，负责共识机制和安全保障；平行链（para chain）负责具体的业务场景。平行链与中继链之间存在出口队列（egress）和入口队列（ingress）两条消息通道。XCMP 协议的工作过程如图 7 所示，具体为：

①链 A 中的用户调用已部署的智能合约，触发一条发往链 B 的跨链消息 *M*；

②链 A 的消息收集者（collator）在收到跨链消息 *M* 后，连同目的地址（address_des）和时间戳（timestamp）等信息放入链 A 的出口队列中；

③链 B 的收集者通过轮询方式发现有一条从链 A 发来的跨链消息 *M*，然后将其放入自己的入口队列中，以待被打包进区块；

④链 A 和链 B 的验证者（validator）分别会接收到跨链消息 *M* 调出和调入队列的消息，并进行验证；

⑤当链 B 的收集者将队列中的跨链消息 *M* 打包进区块时，消息 *M* 会执行链 B 上相应的智能合约，完成资产转移操作；

⑥链 B 中的收集者将新生成的区块（包含有消息 *M*）提交给验证者进行验证，当确认无误后该区块将添加到主链的尾部，跨链操作得到确认。

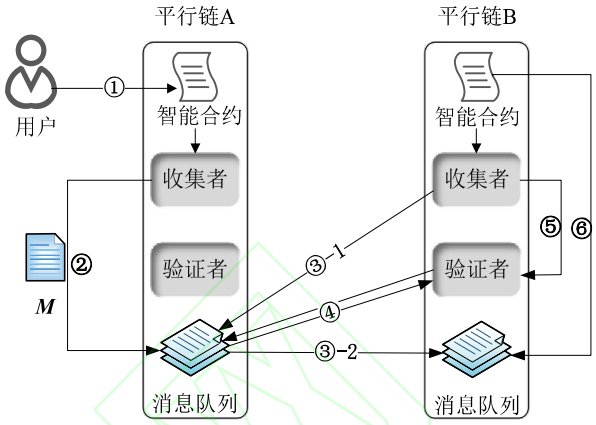

Fig.7 A working diagram of the XCMP protocol

图 7 XCMP 协议工作示意图

（3）IBTP 协议。IBTP（inter-blockchain transfer protocol，跨链传输协议）[56]是一个基于中继链方式的跨链通信协议。IBTP 协议的特征主要表现为：一是跨链交易的合法性验证和交易的路由选择都在中继链中进行，有效提升了协议的安全性；二是可以将跨链网络划分为多个逻辑域，不同域之间通过跨链网关实现交易的多级跨链路由，并支持无状态的跨链消息转发，以此来提升应用的可扩展性和兼容性；三是借鉴 TCP/IP 工作机制，以数据包格式封装消息，并对数据包中的字段进行了严格定义，为跨链操作提供了统一标准和规范，并实现了跨链交易的有序性和可验证性；四是消息经对方公钥加密处理后再进行发送，确保了消息传播的安全性。同时，调用信息经跨链网关间协商的对称密钥加密后再发送到中继链，以此保证传输调用的安全性与可靠性。IBTP 协议应用于 BitXHub 平台。

（4）CCIP 协议。CCIP（cross-chain interoperability protocol，跨链互操作协议）[57] 是为开发人员提供的一个通用的、开放的标准，以构建可以跨多个网络发送消息、传输代币和发起操作的安全服务和应用程序。CCIP 协议正在完善中，将会应用到去中心化的预言机（Oracle）项目 Chainlink 中[58]。Chainlink 项目的目标是开发全球首个去中心化预言机网络（decentralized oracle networks，DON）[59]，其核心功能是以安全的方式实现区块链与链下应用系统（各类 APP）之间的数据交换。在跨链操作中，跨链互操作性使不同的区块链能够相互通信，使智能合约能够通过跨链通信向其他区块链读写数据。来自源链的智能合约调用 Chainlink 的消息路由器，该路由器将利用 Chainlink DON 安全地将消

息发送到目标链，在目标链中，另一个消息路由器验证接收到的消息，通过验证后将其发送到目标智能合约。

（5）LayerZero 协议。LayerZero 协议[60]是一个去信任的跨链互操作协议，通过消息在区块链之间的发送，实现资产、信息、数据和智能合约在区块链之间的交换。顾名思义，LayerZero（零层）位于体系结构的最底层，其主要功能是为实现任何区块链之间的通信提供最基础的支撑和保障。为此，可以将 LayerZero 理解为跨链基础设施，通过部署在每条链上的智能合约实现链间信息的交换和价值转移。如图 8 所示，LayerZero 主要由预言机（Oracle）、中继器（Relayer）和终端（Endpoint）3 个核心组件组成，协议的核心功能是依赖预言机和中继器，在不同链的终端之间传递信息。其中，每条链上部署一个终端，每个终端由一系列智能合约组成，负责与用户或应用程序进行交互，用户端的终端称为应用程序（user application，UA）；预言机是一个独立于 LayerZero 协议的外部组件，目前使用的是 Chainlink，其作用是将区块头信息发送到目标链，然后结合中继器提供的证明信息验证交易的有效性；中继器的功能是获取和传送指定交易的证明信息。

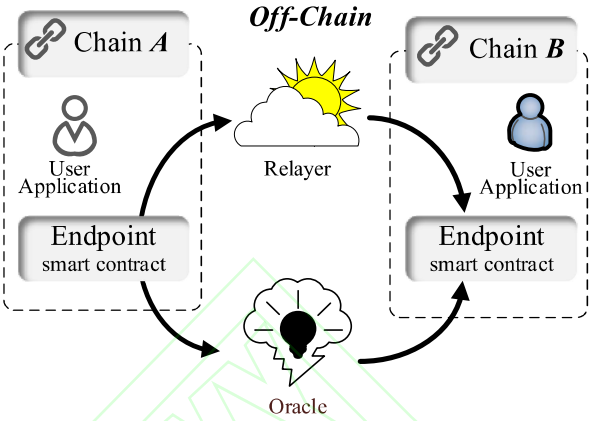

Fig.8　A working diagram of the LayerZero protocol

图 8　LayerZero 协议工作示意图

通过以上分析不难发现，随着区块链跨链场景和应用需求的发展，已有通信协议在迭代中不断得到丰富和完善，与此同时，一批新的通信协议开始以崭新的面貌出现。尤其是随着跨链操作向着纵深发展，实现链上与链下协同、信息网络与价值网络融合成为跨链发展的新需求，区块链预言机（oracle）[61]作为将数据从区块链外传输到区块链上的工具开始引起研究者的重视并发挥其作用。表 6 选择了通信协议的主要特征进行了对比分析。

Table 6　The main performance comparison of different cross-chain communication protocols

表 6　不同跨链通信协议的主要性能比较

通信协议	技术实现	适用范围	安全性	隐私保护	可扩展性	技术复杂性	应用场景
IBC[54]	中继	异构链	较低	未提供	较好	较简单	Cosmos
XCMP[55]	中继/侧链	异构链	高	支持	较好	较复杂	Polkadot
IBTP[56]	中继	异构链	高	支持	较好	复杂	BitXHub
CCIP[57]	预言机	区块链/APP	/	支持	好	复杂	Chainlink
LayerZero[60]	预言机/中继	异构链	较高	支持	好	复杂	Stargate

表 7 给出了 4 个跨链操作技术在性能、公证人机制、侧链/中继、哈希锁定和分布式私钥控制等主要性能方面的比较。

Table 7　The main performance comparison of different cross-chain technologies

表 7　不同跨链技术的主要性能比较

性能	公证人机制	侧链/中继	哈希锁定	分布式私钥控制
互操作性	所有	所有	交叉依赖	所有
安全模型	51%以上的公证人诚实	在链有效的前提下	在链有效的前提下	在链有效的前提下
价值转移	支持（基于信任）	支持	不支持	支持
资产质押	支持（基于信任）	支持	部分支持（难度较大）	支持
多币种智能合约	支持（实现难度大）	支持（实现难度大）	不支持	支持
整体实现难度	容易	难	较容易	较难
原子性	基于公证人	通过智能合约	基于时间锁和哈希锁	基于多重签名算法

通用性	强	较强	不强（仅支持部分链）	较强
安全性	较弱（依赖公证人诚实性）	较弱（依赖矿工的诚实性）	强（依赖哈希算法）	强（依赖多重签名）
信任保障	需要（基于公认人的诚信）	不需要	不需要	不需要
交易效率	低	较低	较高	较低
可扩展性	较差	较强（可平行扩展）	较强（可平行扩展）	强（可平行扩展）
典型应用	InterLedger/Corda	BTC Relay/BitXHub	Lighting Network	Fusion/Wanchain

4 典型跨链应用

根据前文重点讨论的 4 类跨链操作技术和通信协议，结合当前应用和研究实际，一方面突出技术应用和协议规范及功能实现，另一方面体现问题导向和应用示范，本节有针对性地选择以下的典型跨链应用进行分析。

4.1 BTC Relay

BTC Relay 被称为是区块链上的第一个侧链，是由 ConsenSys 推出的基于以太坊智能合约的跨链解决方案。BTC Relay 以一种安全的去中心化方式把以太坊与比特币连接起来，利用带有比特币 SPV 钱包功能的以太坊智能合约，实现了用户在以太坊系统中验证比特币交易。BTC Relay 利用比特币区块头创建一条轻量级的并行链（以太坊的侧链），以太坊 DApp 开发者可以通过智能合约向 BTC Relay 进行 API 调用来验证比特币网络的运行情况。

BTC Relay 的工作过程如图 9 所示，首先中继者（relayer）不断提交 BTC 区块头部数据，然后已提交的 BTC 交易通过验证并支付一小笔费用，最后通过验证的 BTC 交易被发送到智能合约，同时中继者获得一小笔费用的奖励。BTC Relay 的核心是在以太坊智能合约中保存一份完整的以链表方式维护的 BTC 区块头部数据（目前 764331 个区块的总量约为 58.5MB，每年增量为 4MB），区块头部数据由网络中的中继者主动推送。当用户需要验证一笔 BTC 交易的合法性时，只需要提交该交易和 Merkle 路径信息，智能合约即可通过合约中保存的区块头部数据对该笔交易进行快速验证。为了鼓励中继者向 BTC Relay 提供区块头部数据，以太坊智能合约会向提供验证的用户收取费用，而将这笔费用奖励给提交包含这笔交易所在区块的中继者。

严格地讲，BTC Relay 提供的是一套解决 ETH 与 BTC 跨链支付的方案，而且只能将 BTC 引入 ETH，而无法将 ETH 引入 BTC，这种单向解决方案反映出了 BTC Relay 的局限性。

在侧链技术中的另一个典型项目是 RootStock[62]，它是建立在比特币区块链上的智能合约分布式平台，其目的是通过创建一条比特币的侧链，将复杂的智能合约转移到侧链上运行，一方面减轻比特币网络的压力，另一方面扩展了比特币网络的应用。

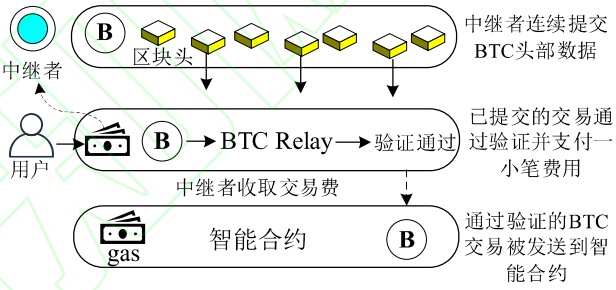

Fig.9 Schematic diagram of BTC Relay

图 9 BTC Relay 工作示意图

4.2 InterLedger

InterLedger Protocol（ILP，账本间协议）是瑞波（Ripple）实验室提出的一个主要采用公证人机制、同时利用了哈希锁定功能的典型项目[63]。Ripple 实验室对 ILP 的目标是兼容所有记账系统之间的差异性，将基于区块链数字货币的支付操作嵌入到 Web 环境中，创建一个统一的网络金融传输协议，使互联网 Web 支付与 ILP 支付走向融合，实现价值互联网（Internet of Value）无处不在的支付功能。

ILP 是一个基于公证人机制的开放协议，实现了两个不同的记账系统之间通过第三方“连接器”（或“验证器”）相互交换货币，而且记账系统之间只需要达成一致而无需事先建立与“连接器”之间的信任。ILP 是一种基于互联网环境的跨越不同区块链系统实现跨链支付的开放跨链操作协议，其中 TCP/IP 协议提供了信息转发和路由功能，而 ILP 提供了资金交易功能。数字支付系统使用分类账（ledgers）来跟踪账户或余额，并支持用户之间的本地转账。连接器可根据实际情况来开发，但必须确保对发送者的资金是安全的[64]。“托管”是 InterLedger 协议实现中的核心功能。根据协议约定，

交易发起方创建“托管”支付地址，并将资产转移到该地址，经哈希锁定后实现资产的临时托管。实现托管的资产最终被确认或退回（拒绝），取决于哈希锁和时间锁，任何参与方只要知道哈希原像就可以做出交易确认或拒绝决定，被托管的资产在时间锁规定时间内得到有效保护，当超时后托管交易自动失效。

例如，Alice 要用自己的比特币（BTC）从 Bob 处购买某一商品，而该商品只能以瑞波币（XRP）定价，在此情况下，Alice 需要借助公证人（连接器）将 BTC 先兑换成 XRP，然后再向 Bob 支付，具体实现过程为（如图 10 所示）：

①Alice 发起交易请求，Bob 生成一个作为哈希原像的“共识密码”s，然后通过加密通道发给 Alice，同时 Bob 将在 ILP 网络中为本次交易创建的支付地址发给 Alice。

②Alice 与“连接器”Trudy 协商，确定 Alice 需要支付给 Trudy 的 BTC（其中包括 Trudy 收取的手续费）数据。

③根据 ILP 协议要求，Alice 生成 ILP 数据包，其中目标地址指向 Trudy，并对从 Bob 处获得的“条件原像”s 计算其哈希值，即 h=hash(s)，将结果 h 打包进 ILP 数据包。

④Alice 在比特币账本系统发起并创建一个“托管”操作，其中将 h 作为托管条件，并设置一个超时时间 t_1。

⑤Trudy 在比特币系统监测到一个有关自己的“托管”操作。

⑥Trudy 解析 ILP 数据包，得知自己应向 Bob 支付的 XRP 数量。然后生成一个 ILP 数据包，发送给 Bob。

⑦Trudy 在瑞波账本系统上发起并创建一个“托管”操作，其中将 h 作为托管条件，并设置一个超时时间 t_2（$t_2 < t_1$）。

⑧Bob 在瑞波系统上监测到一个有关自己的“托管”操作。

⑨Bob 解析 ILP 数据包，得到 h 和交易金额，然后计算本地原像 s 的哈希值，如果结果与收到的 h 相同，则确认“托管”交易，否则拒绝本笔交易（本例假设确认托管交易）。

⑩Bob 在瑞波账本系统上发起一个“托管”确认操作，Bob 收到相应数量的 XRP。

⑪Trudy 在瑞波系统上监测到一个有关自己的“托管”确认操作。

⑫Trudy 解析“托管”确认操作内容，得到“条件原像”s。

⑬Trudy 在比特币账本系统上发起一个“托管”确认操作，确认“条件原像”s，比特币账本上的“托管”交易完成。

⑭Alice 在比特币账本系统上监测到一个涉及自己的“托管”确认操作，确认该操作，完成交易。

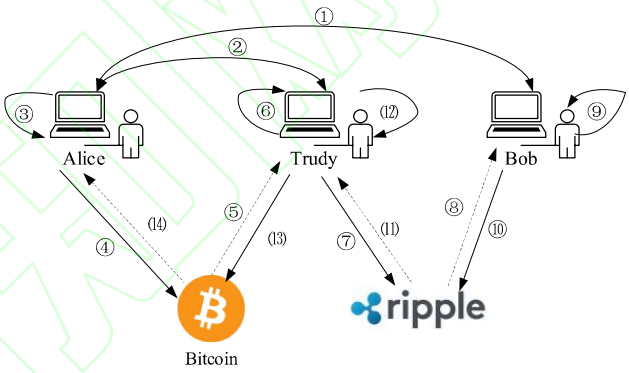

Fig.10 ILP execution example

图 10 ILP 执行示例

4.3 BitXHub

BitXHub 是趣链科技研发的采用 IBTP 协议实现同构及异构区块链间跨链交易的开源跨链服务平台[65-66]，是联盟链中采用“中继链+跨链网关”技术的跨链操作机制，主要由中继链、跨链网关和应用链 3 部分组成，跨链架构如图 11 所示。

（1）中继链（relay-chain）。中继链作为应用链的侧链，是一个基于 IBTP 跨链协议的开放许可链，负责跨链交易的可信验证与可靠路由，确保跨链交易的事务一致性。BitXHub 通过中继机制提供跨链交易信息的监测、获取、验证和传递等功能，实现系统的安全服务。中继链与应用链之间组成联盟链关系，应用链中的节点通过相应共识机制共同参与中继链的维护。所有跨链交易信息永久保存在中继链的账本中，以备实时查询。

（2）跨链网关（pier）。从网络互联方式看，跨链网关类似于互联网网关，只是互联网网关主要负责不同网络间信息的交换，而跨链网关担负着区块链间收集、验证和传递交易的角色。跨链网关一般由应用链和中继链中相应的服务程序维护，既可

以用于应用链与中继链之间的互联，实现应用链接入跨链系统，也可以用于中继链之间的连接，以扩展中继链的连接范围。BitXHub 提供跨链网关插件（plugin）机制，将跨链网关中与应用链交互的模块与网关的核心功能模块解耦，以便于应用链接入跨链系统。

（3）应用链（app-chain）。应用链负责具体的业务逻辑，承载不同场景下的具体应用。应用链与直连中继链之间的关系分为同构链和异构链两种类型，其中当应用链直接支持 BitXHub 规范，且两者的区块和交易数据结构类似，同时共识机制相同时为同构链，否则为异构链。相对于异构链，同构链之间的连接要简单许多。为了完成跨链操作，需要在应用链上部署跨链管理合约（broker）和业务合约，其中 broker 负责对接跨链网关，而业务合约负责对接具体的业务场景。跨链业务合约是业务合约中的一种特殊的合约，主要负责将所在应用链中的跨链请求提交到 broker 上。

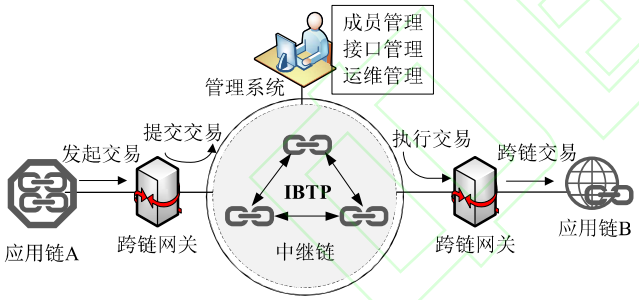

Fig.11 BitXHub cross-chain architecture diagram

图 11 BitXHub 跨链架构图

另外，BitXHub 还通过管理系统实现对跨链操作的全过程管理，主要包括对应用链成员的审核、对交易状态和跨链合约相关模板界面等操作的管理以及实时监控和展现系统的运行状态等。

区块链的封闭性导致难以实现与外界的信息沟通与交流。为了使中继链能够以开放方式进行跨链消息的验证和路由，让跨链网关能够以标准模式进行跨链消息处理，BitXHub 设计了类似 TCP/IP 的 IBTP 跨链协议。IBTP 跨链协议通过跨链服务实现不同应用链上业务之间的交互，通过跨链消息证明和信任树保证跨链消息的有效性以及实现对跨链消息的合法性验证。IBTP 报文采用 P2P 方式进行传输，报文中封装的内容均采用对方的公钥进行了加密，确保传输的安全性。报文在跨链网关之间传输时，经双方协商生成的对称密钥加密，保障了数据的安全性和可靠性。

以单一中继链跨链架构为例，所设应用链 *A* 中的用户 Alice 要向应用链 *B* 中的 Bob 进行转账，BitXHub 跨链交易的简易流程为（如图 12 所示）：

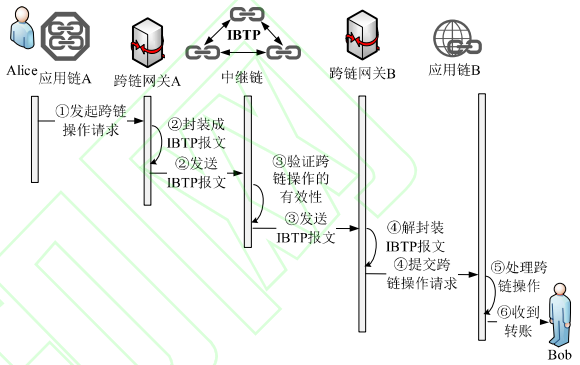

Fig.12 BitXHub cross-chain operation simple process

图 12 BitXHub 跨链操作简易流程

①Alice 发起跨链转账请求，应用链 *A* 中跨链业务合约调用跨链管理合约（broker），向跨链网关 *A* 发送跨链操作请求。

②跨链网关 A 中的插件（plugin）捕捉到请求，将该请求提交给网关核心模块进行处理。网关核心模块把跨链操作请求封装成相应的 IBTP 报文，然后交给中继链。

③中继链对应用链 *A* 的跨链操作请求的有效性进行验证，通过验证后将其提交给跨链网关 *B*。

④跨链网关 *B* 将接收到的 IBTP 报文解封装，将得到的跨链操作请求提交给应用链 *B* 的 broker。

⑤应用链 *B* 的 broker 将跨链操作请求提交给跨链业务合约。

⑥跨链业务合约上的用户 Bob 将收到来自应用链 *A* 的 Alice 的转账。如果系统对跨链交易结果需要时行回执，则逆向执行前面的过程。

根据 BitXHub 白皮书描述，接入中继链的应用链数量一般不超过 64 个，所以在较大的跨链生态中需要由多个中继链组成的中继链链联网来连接不同的应用链，不同中继链的网关之间采用 P2P 方式通信。

4.4 Lighting Network

作为加密数字货币的经典应用，比特币虽然以其创新理念和创世应用取得了巨大成功，并正在改变着传统的组织管理模式，但其存在的难以扩容、

交易难以即时确认以及呆板的收费模式等问题严重制约着比特币系统应用向着纵深发展，尤其是高频、小额这类日常生活中最普遍的应用，却是比特币系统最难以胜任的应用场景。为了解决上述问题，支付通道技术和支付通道网络（payment channel network，PCN）[67-68]应运而生，随后，PCN 开始应用到闪电网络（lightning network，LN）[69]，并部署到比特币系统上。

（1）支付通道和支付通道网络。作为解决比特币系统可扩展性问题的一种有效方案，支付通道（或称“微支付通道”）将部分不易于链上进行的交易转移到链下，交易双方只需要在开启和关闭支付通道时与区块链交互，其他交易可通过支付通道在链下快速并以廉价方式进行。支付通道提供了链下一对一的高效支付能力。支付通道的运行主要包括通道开启、链下交易和通道关闭 3 个过程。

①通道开启。在区块链上，交易双方通过协商创建一个用于存放双方抵押金的交易地址（funding transaction），该地址为一个 2-of-2 多重签名地址，其中的抵押金只有在交易双方共同签名后才能取回。交易双方通过创建的 funding transaction 地址构成了一个双方共享的支付通道，当某一支付通道创建后，每一笔交易的实质便是用户余额之间的变动。

②链下交易。交易双方在已构建的支付通道中进行线下交易，根据交易需要，交易在支付通道中既可以是单向进行，也可以双向进行。其中，RSMC 为任意两个用户之间的交易提供安全保证，当交易的任意一方试图通过作恶获取非法收益或进行双花消费时，RSMC 将通过惩罚机制将作恶方当前的余额全部转给另一方。交易细节仅限于通道内，所有交易痕迹都不会上链。在支付通道内，双方可以进行多次交易，在每次交易（余额变动）中，双方都会生成新的交易地址用于存放各自的余额，并采取多重签名机制保证交易的安全性，当一笔新交易产生时，前一笔交易会进行多重签名而自动失效。

③通道关闭。当双方不再进行链下交易并对最终交易结果达成共识后，将在区块链上交换彼此的签名，funding transaction 地址在通过有效的 2-of-2 多重签名后，双方取回各自的抵押金，支付通道自动关闭。

在区块链基础上，随着支付通道数量的增多，形成了由众多参与节点与支付通道组成的网络，即支付通道网络。利用支付通道网络，参与者可以将其他支付通道作为中继进行跨通道多跳支付。

（2）闪电网络。闪电网络借助支付通道技术实现了对比特币系统的链下扩容，其中比特币系统作为主链，扮演着第三方仲裁机构的角色，负责为交易双方提供开启和关闭支付通道的功能。

闪电网络引入了支付通道网络功能，并通过 HTLC 协议解决多跳支付转发的问题。在闪电网络中，多数情况下，交易双方之间一般不存在直接支付通道，而是利用支付通道网络借助其他已经创建的支付通道进行跨通道多跳支付。如图 13 所示的是闪电网络中单一路径上的支付转发操作示意图，其中 HTLC 协议实现了多跳交易的原子性，即在多跳支付转发过程中，只有在每一跳支付转发全部按要求完成后，涉及到该交易的所有支付通道的余额变动都会更新，然而，一旦某一跳没有顺利完成，则宣告本次交易失败，所有涉及到的支付通道中的余额变动仍然保持在前一次的状态。

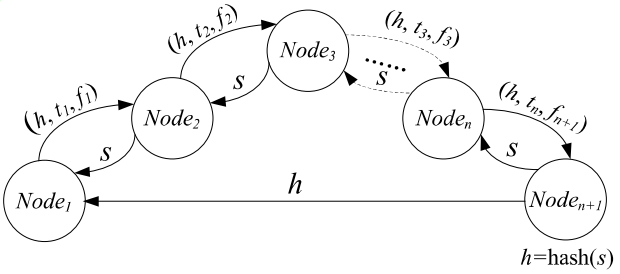

Fig.13　Single path payment forwarding diagram

图 13　单一路径支付转发示意图

闪电网络充分应用了 HTLC 的哈希锁和时间锁功能，其中哈希锁实现了支付转发的不可否认性，而时间锁规定了具体交易的有效时间。在图 11 中，正向转发的每一跳信息由哈希值 h（h=hash(s)）、时间 t_i(i=1,2,3, …，且 t_i>t_{i+1}) 和交易收费 f_i(i=1,2,3,…)(每个节点收到的费用可能相同，也可能不同）组成，而返向通道中转发哈希原像 s。交易接收方节点生成一个随机数作为哈希原像 s，计算哈希值 h=hash(s)，将 h 发送给交易发起方节点；正向支付转发路径上的所有节点都会获得 h，只有当交易接收方节点在有效时间内将 s 提交给上一跳的转发节点时，才开始解锁操作过程，并获得交易合约中的资金。此过程是哈希锁的应用，下一步将

由时间锁发挥其功能。由于每一笔支付转发交易都设置了一个有效时间，如果在有效期内转发节点没有收到下一跳接收节点提交的原像 s，则交易合约中的资金便会因为超时而被退回给转发节点，确保了交易过程中资金的安全性。

4.5 Wanchain

Wanchain（万维链）由一批密码学专家和资深区块链工程师组成的团队开发，具有跨链功能的Wanchain2.0 于 2018 年 7 月 23 日上线，并首次实现了与以太坊之间的对接。Wanchain 是采用分布式私钥控制技术的公有链跨链项目[70]，跨链操作参与方将各自的代币锁定在一个只有多方协同才能够操作的共享账户内[71]，每个节点拥有私钥的一个片段，如果要对该共享账户进行操作，需要有一定数量的节点达成共识，从而创建了一个真正去中心化和可互操作的区块链广域网络。Wanchain 是一个基础的分布式区块链互操作性解决方案，提供了一个完全类似以太坊的环境，验证节点（validator nodes）之间使用一种称为星系共识（galaxy consensus）[72]的专有权益证明（proof of stake，PoS）[73]共识算法，该共识算法利用了分布式秘密共享、门限签名等多种签名技术，以优化随机数生成和块生成机制。

Wanchain 是一个基于以太坊的实现不同区块链网络之间互联互通的分布式账本，支持主流公有链、私有链、同构链、异构链之间的跨链交易。Wanchain 在以太坊常用交易方式的基础上，通过环签名方案和一次性账户方案增加了隐私保护机制。当区块链需要与 Wanchain 集成时，首先要在 Wanchain 上进行资产注册，以确保被唯一标识。对于跨链交易，使用安全多方计算（secure multi-party computing，SMPC）和门限密钥共享机制（hreshold secret-sharing schemes），在不改变原始链运行方式的情况，以最小成本实现了跨链操作。更为重要的是，接入 Wanchain 的区块链相当于 Wanchain 的同质区块链，具有相同的跨链机制，彼此之间可以进行高效对接。

如图 14 所示，下面以以太坊用户 Alice 向 Wanchain 转移资产为例介绍 Wanchain 的跨链操作过程。其中，Wanchain 平台的代币为 Wancoin（WAN）。

Step1:Alice 在以太坊上使用 Wanchain 钱包利用自己的账户 OriAccount 发起交易请求 OriTx，向 Wanchain 的锁定账户（locked account）发送资产 OriAssetID，并通过跨链交易模块向 Wanchain 广播跨链交易请示 InterTxReq。

Step2:Wanchain 中的交易验证节点（voucher）在接收到该跨链交易请求后，验证该交易发起方的合法性和真实性，然后以 OriTxInfo（交易请求信息）、OriChainID（原始链身份）和 OriAssetID 作为 TLF（token locked flag，代币锁定标记）函数的输入值，判断其结果的正确性。

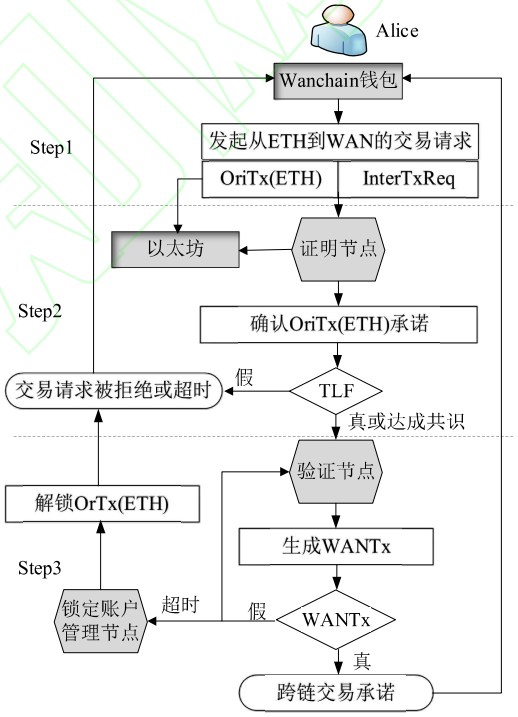

Fig.14 Cross-chain data process from Ethereum to Wanchain

图 14 从以太坊向 Wanchain 的跨链数据交易过程

Step3:跨链交易证明节点对收到的 TLF 结果进行判别，如果其值为真，则 OriTx 被确认，同时验证节点（validator）检查以太坊的资产注册情况。如果是一个新资产，将被添加到资产注册中心。此时，由验证器维护的公共账户 WANAccount 发起交易 WANTx，为新添加的资产部署智能合约，并在合约中为 OriAccount 分发价值代币。如果是已经注册的资产，交易 WANTx 将价值代币直接分配到现有的资产合约中。在确认了 WANTx 后，验证节点 validator 使用跨链交易数据传输模块向 Alice 回复跨链交易成功信息。如果 WANTx 无效，锁定帐户管理节点（storeman）在以太坊上发起一个交易，

将 Alice 的锁定资产转移回 OriAccount；如果 TLF 的共识结果被证明节点确认为假，则认为跨链交易无效。

如果将资产从 Wanchain 转回原始链（如以太坊），其思路与前文介绍的从原始链转向 Wanchain 类似，技术细节略有不同。2021 年 2 月 26 日发布的 Wanchain5.0 新增了“质押金共享式多链互跨”机制，即所有进行跨链操作的区块链共享同一个押金池，在有效降低了跨链操作复杂度的同时，提高了跨链的便捷性、安全性和可扩展性。同时，在“质押金共享式多链互跨”机制中还成功实现了“直连桥”模式，即加入 Wanchain 的区块链之间无需扮演路由角色的 Wanchain 就可以直接实现资产的转移。

针对前文讨论的跨链操作技术和通信协议，本节分别选取了有代表性的应用场景进行了较为系统的分析。在此基础上，表 8 从跨链技术、跨链认证、原子交易、资产质押、智能合约部署的难易度、信任模型、交易效率和安全性等方面对各应用场景进行了对比分析。其中，跨链认证用于实现不同区块链之间的身份认证功能，在较大程度上决定着系统的安全性和隐私性；原子交易是区块链跨链操作的核心技术，用于实现运行在不同区块链上的交易要么全部完成，要么全部取消。原子交易可以有效防止交易用户间发生欺诈行为，保证交易的安全性；资产质押是区块链中以数字资产作为抵押来获得身份或权力并确认交易的过程，质押可保证只有合法的信息和交易被添加到区块链，以提升交易的安全性和系统的可靠性；智能合约是跨链操作中使用的主要技术手段之一，其部署方式和难易程度在较大程度上决定着部分跨链功能的实现；信任模型是以信任为基础的区块链工作模式，影响着跨链操作的实现方式和性能。

Table 8　Comparative analysis of performance in typical cross-chain application scenarios

表 8　典型跨链应用场景性能对比分析

应用场景	跨链技术	跨链认证	原子交易	资产质押	智能合约部署	信任模型	交易效率	安全性
BTC Relay	侧链	不支持	无法实现	不支持	较容易	主链+侧链	较低	较好
InterLedger	公证人	支持	可实现	支持	较为困难	51%公证人诚实	低	较差
BitXHub	通信协议	支持	可实现	不支持	较为容易	中继链+跨链网关	较高	较好
Lighting Network	哈希锁定	不支持	可实现	部分支持	不支持	链的有效性	较高	较好
Wanchain	分布式私钥控制	支持	可实现	支持	容易	链的有效性	高	好

5 跨链操作的安全问题

从总体上看，现有的跨链操作协议和项目大都是基于前文介绍的跨链技术和通信协议来实现，而每种技术或通信协议其自身存在不同程度的安全风险。另外，由于区块链系统自身所具有的价值属性，构建于传统数据通信网络环境中的区块链系统，其本质上不利于跨链操作的实现，现有的一些跨链机制和项目一般是以牺牲安全性来换取互操作性。为此，本节将结合具体技术、通信协议和应用场景，对跨链操作中存在的主要安全问题进行分析。

5.1 跨链技术的安全性问题

跨链技术是实现区块链互操作的核心。随着区块链技术的不断演进和应用的快速推出与迭代，使跨链操作变得越来越复杂，复杂性很大程度上引发了安全问题。

（1）公证人机制的安全问题。公证人机制具有高效灵活地支持不同数据结构和不同共识机制区块链之间支付的优点，在跨链操作领域得到了广泛应用。与此同时，公认人机制因中心化产生的安全问题也突显出来。公证人机制中资产交换的核心是作为公证人的第三方机构，其安全性主要依赖于第三方机构的可信性和公证人的诚实性，虽然采取多重签名和公布式多重签名等机制克服了单签名机制存在的安全问题，有效提升了系统整体的安全性，但中心化机制本身就与区块链技术的初衷相违背，中心化程度越高安全性越差。如果要提高去中心化程度，就需要以牺牲系统的性能为代价。例如，典型的基于公认人机制的项目 InterLedger，其功能主要通过驻留在主机或连接器中的 InterLedger 模块来实现，基于 InterLedger 地址进行账本之间的路由支付。由于公认人的中心化机制，当攻击者控制了主机或连接器节点后，就可以通过修改 ILP 支付包格式实现虚假支付。同时，还可以通过嗅探方式

监听不同 InterLedger 地址的通信情况。针对此问题，InterLLdger 项目后来采用了闪电网络中使用的 HTLC 技术，以降低系统的中心化程度，并有效实现交易的原子性。

（2）侧链/中继的安全问题。侧链与主链之间的安全机制相互独立。由于侧链通常为特定类型的交易而设计，其共识算法一般不会直接继承主链的安全属性，交易的安全性无法得到主链的监管。中继作为主链的抽象层和通信中枢，需要收集各区块链之间的数据并通过获得区块头部的有效信息进行交易验证和消息转发，所以中继对收集和获取全网信息的能力有限，从而无法利用中继机制分析和判断违规交易（如双重支付）的发生。同时，相对于主链而言，侧链/中继节点的数量有限，抵御 51% 攻击的能力较弱，而且侧链/中继机制严重弱化了区块链去中心化特征，参与侧链或中继共识算法的节点的诚实性决定着跨链操作的安全性。例如，2022 年 3 月，Axie Infinity 的以太坊侧链 Ronin Network 的跨链网桥受到攻击，其中 9 个验证者中有 5 个的私钥被盗。2022 年 6 月，由公链项目 Harmony 开发的跨链桥 Horizon Bridge 的私钥同样被攻击者盗取，而 Horizon 仅要求由 2 个验证者同时提供验证能力。两起安全事件均造成不小的损失，而究其根源在于整个系统高度依赖于数量非常有限的趋于中心化机制的验证节点。

（3）哈希锁定的安全问题。哈希锁和时间锁是哈希锁定的核心，其技术实现高度依赖于哈希原像的安全性和资金锁定时间的合理性。从算法实现角度看，哈希锁的安全性取决于在哈希算法和哈希值已知的前提下如何获得原像的能力，即抵御“原像攻击”（preimage attack）[74]的能力。当然，在哈希锁定机制中，接收节点在随机生成原像时，原像的复杂性和文件大小，同样决定着系统的安全性和运行性能，为此，需要在安全性与系统性能之间进行权衡。每一笔交易都通过时间锁设置一个用于限制交易有效期的锁定时间，发送者（或转发者）如果在有效期内未收到接收者（或下一跳节点）提交的原像，则交易合约中锁定的资金将被退回。值得注意的是，锁定时间的设置必须合理，尤其是多跳转发路径上不同节点锁定时间的设定更需要考虑系统性。否则，节点可能会因锁定时间设置的不合理而导致资金的损失[75]。哈希锁定的典型应用场景是闪电网络，而 PCN 是闪电网络实现链下支付的主要方式，大量支付通道的创建和应用如果失去了有效监管和控制，将会对系统安全和隐私安全造成重大威胁[76]。

（4）分布式私钥控制的安全问题。分布式私钥控制机制类似于公证人机制，只是与存储资产对应的私钥采用分布式存储方式，从而克服了公证人机制中心化带来的安全风险。多方计算和门限密钥等技术构建了分布式私钥控制的密码学基础，对分布式私钥控制的安全性起着决定性作用。分布式私钥控制机制的另一个安全问题集中于私钥管理。由于分布式私钥控制机制是将针对某个数字资产的私钥分成 N 份私钥片段后分发给网络中的 N 个不同的验证者分别保存，在需要对锁定的资产进行解锁时，只需要从 N 个验证者中分别得到 K（$K \leqslant N$）个验证者保存的私钥片段，并经重组后就可以恢复出一个完整的私钥。由此可以看出，M 和 K 值的大小在很大程度上决定着私钥的安全性。例如，在前文介绍的 Ronin Network 案件事件中，M 和 K 值分别只有 9 和 5，而 Horizon Bridge 案件事件中的 K 值只有 2。在安全事件发生后，两个项目分别增加了验证节点的数量，例如 Ronin Network 计划在 3 个月内将验证节点增加到 21 个，然后继续增加到 100 个。

（5）跨链通信协议的安全问题。体系结构和通信协议是计算机网络的两大核心和支柱，区块链系统也不例外。跨链通信协议的安全问题主要来自于协议内生的安全问题、多协议混合过程中出现的安全问题以及协议实现中出现的安全问题 3 部分。其中，协议内生的安全问题主要是指协议设计存在的缺陷，是普遍存在和不可避免的。但是，与信息网络不同的是，作为价值网络的区块链系统具有其安全的特殊要求，有一些区块链应用就是因为协议中存在的功能和安全缺陷导致昙花一现的命运；多技术、多协议混合过程中出现的安全问题更为复杂，例如首个采用 DPoS（delegated proof of stake，委托权益证明）共识机制的跨链 3.0 项目 Ether Universe[77]，同时采用了公证人和侧链混合机制，从而增加了多币种智能合约设计和部署的复杂性，也为系统安全性的实现提出了更多挑战；协议实现中的安全问题直接映射到应用软件的安全问题，例

如，2016 年 6月发生 the DAO 事件[78]，就是利用了以太坊智能合约调用外部合约时存在的安全漏洞实现的重入 (re-entrance) 攻击，最终直接导致了以太坊硬分叉，分为 ETH 和 ETC。

5.2 跨链操作过程中产生的安全问题

区块链跨链操作过程中产生的安全问题是一个衍生问题，也是一个共性问题。区块链跨链操作过程中产生的安全问题主要表现在以下几个方面。

（1）孤块。孤块（orphan block）[79]是指在挖矿过程中临时产生的区块，因其与账本形成机制之间产生冲突，所以最终不会存在于主链上。孤块是缺乏竞争力的合法区块。在分布式网络中，因受网络连接距离、带宽等因素的差异性影响，致使节点之间存在不同的网络延时，这为区块链网络尤其是公有链网络共识结果的形成带来了不确定性，尤其在采用 PoW 共识机制的区块链网络中，一个区块最终能否上链需要等待较长一段时间（如比特币系统需要等待 1h）。但是，对于一个区块链网络来说，可能会在同一时间内发布多个区块，这将导致同一区块链在任意时刻可能存在不同版本的多个账本。然而，区块是否被账本最终接受通常是基于概率的，而不是确定的，因为区块可以被取代，最终没有成功上链的区块将以孤块的形式被丢弃。在跨链操作过程中，某个数字资产已经从原始链转移到了目标链，但受原始链共识机制的影响，包含该数字资产的交易所在的区块最终以孤块形式被丢弃，这将导致在目标链上“凭空”出现了新资产，从而使跨链操作出现混乱。

（2）重放攻击。区块链出现硬分叉后，将存在原始链和分叉链两条并行运行的区块链，如 BTC（比特币）和 BCC（比特币现金）、ETC（以太经典）和 ETH（以太坊）等。根据硬分叉产生的机制，原始链和分叉链可能具有完全相同的交易格式、数据结构、交易地址空间和公钥密钥算法，所以在原始链上发生的交易可能在分叉链上也会合法发生，反之亦然。攻击者只需要将其中一条链上发生的交易信息复制到另一条链上，并在两条链上分别得到确认，从而发起重放攻击（replay attack）[80]。如果重放攻击发生在跨链操作过程中，将会导致同一笔跨链交易在原始链和分叉链上同时发生并得到有效确认，造成被攻击者资产的损失。

（3）日蚀攻击。P2P 网络在分布式网络环境中为节点之间提供了一种自组织的组网模式，为区块链系统提供了公平的底层通信能力。但是，P2P 网络在身份认证、数据合法性验证、网络安全管理机制等方面存在的先天性缺陷或不足，为攻击者实施 DDoS（distributed denial of service，分布式拒绝服务攻击）[81]、日蚀攻击（eclipse attack）[82-83]等网络攻击行为和进行木马、蠕虫等各类恶意代码的传播提供了温床。可以通过网络嗅探或监听等方式来确定 P2P 网络中节点之间的拓扑结构，进而搜索和定位被攻击的目标节点。日蚀攻击便是攻击者在确定了节点之间的网络拓扑后，对目标网络或节点实现隔离的一种典型攻击方式。其基本思想是在确定了目标节点后，将借助 P2P 网络工作机制（如 TCP 同时连接数限制），屏蔽目标节点与其他节点之间的通信，甚至在对目标节点实施隔离后，使其只能接收到攻击节点的信息，从而使目标节点中存放的账本出现与主链账本不一致的现象。在跨链操作过程中，攻击者利用日蚀攻击破坏跨链操作的有序进行，甚至迫使某些节点无法进行跨链操作。

（4）长距离攻击。长距离攻击（long range attrack）[84]是指攻击者在某个区块高度（也可能是创世纪区块）开始，使用区块链现有账本信息和代币余额来创建一个与真实链难以区分的恶意分叉链，然后欺骗用户使其在恶意分叉链上进行交易的一种欺骗性攻击行为。采用 PoS 共识机制的区块链中更容易受到长距离攻击的威胁[85]。如图 15 所示，长距离攻击的基本实现过程是：攻击者通过各种手段（窃取或购买）获取用户账户的私钥，只要这些用户账户在历史上（如区块 X）曾经拥有过 50%以上的 PoS 权益，就可以在该区块的基础上利用 51%攻击手段进行恶意分叉[86]，制造出一条恶意分叉链。与 PoW 共识机制不同，PoS 共识机制没有出块之间的强制延时机制，所以攻击者可以在短时间内产生大量的区块，使恶意区块形成的链超过原始链，从而打破了 PoS 共识机制原有的分叉和防篡改机制。长距离攻击会导致交易在跨链操作中出现双花（double-spend），也可使智能合约因无法进行回滚而不能正常执行。

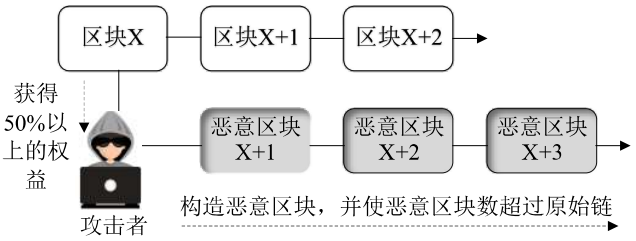

Fig.15 Schematic diagram of long range attack principle

图 15 长距离攻击实现示意图

（5）无权益攻击。无权益攻击（nothing at stake attack）[87]是另一种针对 PoS 共识机制的攻击方式，是指当 PoS 区块链出现分叉时，攻击者会选择同时在原始链和分叉链上同时进行挖矿，以获取最大收益。很显然，无权益攻击违反了 PoS 共识机制。与长距离攻击一样，在跨链操作中无权益攻击同样会导致交易的双花。可以通过设置惩罚机制来防范无权益攻击的发生。

6 总结与展望

6.1 互操作性是确保区块链稳健发展的基础

区块链缺乏先天的互操作性保障。区块链取得今天的巨大成功得益于其实现方法的多样性，即区块链作为一项底层技术或开发平台其自身的异构性。然而，不同技术路径或平台实现在数据结构、共识算法、治理方案等方面存在较大差异，导致区块链不同应用之间相互独立，缺乏互操作性，制约了大规模的跨平台应用。为此，现有的区块链系统在互操作性方法存在着先天不足：

（1）区块链自身是一个相对封闭的系统。不同的区块链使用了不同的身份认证、共识算法、数据结构、代币等方式，如何实现不同系统之间的身份互认、共识互通、数据共享、代币共识，进而实现治理协同，目前在不借助于链外功能的前提下几乎是不可能实现的。

（2）区块链应用缺乏开放性。对于不同的应用来说，区块链仅仅提供的是底层服务，不同的应用会根据具体要求选择不同的底层服务，由于底层服务之间的差异性，使得上层应用无法实现平台之间的平滑转移。

（3）链下数据的可信性、安全性和合规性难以得到保障。区块链利用网络资源、存储资源和计算资源来实现数据的安全性，本身只是一个轻量级的应用。然而，在现实应用场景中，对网络带宽、节点存储和计算能力要求较高的重量级业务（如音视频处理、机器学习、大数据分析等）需要与区块链之间建立关联，从而实现链上链下的互动，进而提升轻量级区块链对重量级业务的支持能力，所以区块链应用的延伸离不开对链下数据、计算及存储能力的合理利用。针对链下数据在处理和交互过程中无法保证其可靠性、安全性和合规性问题的需要，目前已出现了基于 Oracle（预言机）[88]的解决方案，但在工程实现中，还需要从接口规范、通信标准等方面进行约束，从数据安全、隐私安全、内容安全等方面寻求技术突破，以提升区块链系统与链下数据的交互能力。另外，区块链提供的账本数据只能确保线上交易的可靠性和不可否认性，但当存在链上链下互操作（如由链下事件触发链上合约的运行）时，如何实现对链下数据来源、数据传输、数据处理等方面的管理，进而实现链上链下数据协同的可信性，目前缺乏相应的解决方案。

6.2 跨链操作是区块链发展的必然选择

沿着区块链的发展，2009 至 2016 的典型代表是比特币，2017 年开始以太坊通过智能合约快速扩展了区块链应用，2018 年的典型代表是被称为区块链 3.0 主要竞争者的 EOS（enterprise operating system，企业操作系统），从 2019 年开始，区块链在历经了十年发展后终于来到了“万链互联”的初始阶段，其中最具有代表性的便于 Cosmos 和 Polkadot。在目前的跨链技术中[89]，较为成熟的有基于 BTC 的闪电网络、在 ETH 上实现的侧链以及一些跨链项目，但这些跨链技术的实现更多的是通过双向锚定或是原子交换来进行价值在不同区块链之间的转移，其实现功能简单，而且多局限于在已有区块链之间的操作，缺乏通用性、可移值性和可扩展性。在已有的跨链技术中，Cosmos 和 Polkadot 标志着以通过通信协议生成区块链的“万链互联”时代的到来，两者都提供了生成新链的工具（Cosmos 的区块链生成工具为 Cosmos SDK，Polkadot 的区块链生成工具为 Substrate），两者都给予区块链开发者提供了“快速造链”的能力，通过这些协议或标准规范来生成的区块链，在兼容性、可扩展性和互操作性等方面天生具有优势。同时，以 Cosmos 和 Polkadot 为代表的跨链协议为已有的区块链项目也提供了接入方法。

由于区块链本身的特征和丰富的应用，对于链联网的发展和预期，无法出现类似于 Internet 的发展的路径和结果，TCP/IP 协议栈为异构网络之间的互联提供了遵循和标准，而目前几乎不可能提供一个类似于 TCP/IP 的适用于不同区块链之间互联互通的普适性的规范和体系，未来最有可能的发展途

径是分两步走：第一步是构建“同构”链联网。以比特币、以太坊等主流原始链为基础，将通过硬分叉生成的分叉链或通过代码修改生成的新链分类归属于原始链的范围，从而形成同构区块链，这些同构链之间可以通过侧链、哈希锁定、中继、公证人机制等方式进行互联，进而形成同构链联网；第二步是构建真正意义上的链联网。在同构链联网的基础上，通过开发类似于 TCP/IP 的协议栈，为不同区块链之间的互联提供统一的跨链通信协议、实体、接口和服务，进而更大范围的形成真正意义上的链联网。

6.3 价值守恒和不可信验证是跨链操作的两大挑战

目前，跨链操作处于初步的探索阶段，既要考虑已有主流区块链项目之间的互操作性，还要面对新应用对价值转移和信息交换的要求，尚缺乏一种类似于 TCP/IP 的普适跨链操作机制。现存和演进中的任何一个跨链解决方案都必须同时解决两个问题：价值守恒和不可信验证[66,86]。所谓价值守恒是指在跨链操作完成后，虽然发生了价值在不同区块链之间的转移，但每一个区块链上产生的代币数量不会发生变化，同时，在目标链上可用的价值在原始链上将不可用，即价值是唯一的，并可以在不同区块链之间进行转移；所谓不可信验证是指所有交易过程都是利用共识算法在不可信网络环境中完成验证操作，而且跨链操作的验证过程不能影响、更不能修改区块链原有的共识机制。

解决价值守恒的关键是确保交易的原子性以及实现资产的有效锁定。例如，在 Wanchain 中，对于发生的每一笔交易，Storemem 节点都会创建一个无限期持有从原始链转出资金的锁定账户，同时在目标链上以对应映射代币的形式提供等价的资产。然后，只有当对应映射代币的价值返回原始链时，原始资产才能被释放，同时，映射代币被销毁。

解决不可信验证问题的关键仍然是矿工的诚实性问题。由近期发生的一系列安全事件可以看出，如何防止验证者作恶成为跨链操作面临的一大安全挑战。例如，在侧链机制中，无论验证者是由侧链自行选举并管理（如 Cosmos），或由主链确定（如 Polkadot），都会面临验证者不可靠这一根本问题。在具体交易过程中，当实际交易量远大于验证者交纳的押金时，将会对验证者产生极大的诱惑，进而发生作恶行为。现有的跨链方案中，验证者一般采用默克尔树（Merkle Tree）证明方式，即侧链在生成一个新区块时，首先会生成一个针对当前区块所有交易产生状态的状态根（State Root），生成的状态根在得到验证者的签名后保存在当前区块中。这样，在进行交易之前，验证者只需要通过验证状态根就可以验证跨链操作的合法性。当验证者作恶时，只需要基于当前区块联手伪造一个状态根，从而窃取用户锁定在主链上的资产。为此，如何针对具体的跨链操作场景，进一步在去中心化、可扩展性和安全性这一区块链不可能三角之间取得平衡，同时发挥主链对侧链的监管作用，将是下一步跨链操作研究的重点。例如，可设置主链对侧链的监管机制，实时监测侧链上当前区块生成的状态根与验证者提交的状态根之间的异同，以此来判断验证者是否作恶。

参考文献：

[1] WANG Q, LI F J, WANG Z L, et al. Principle and core technology of blockchain[J]. Journal of Frontiers of Computer Science and Technology,2020,14(10):1621-1643.
王群,李馥娟,王振力,等.区块链原理及关键技术[J].计算机科学与探索,2020,14(10):1621-1643.

[2] NFTing.Cross-Chain Technology: The Future of Blockchain Interoperability[EB/OL].(2020-05-24)[2022-09- 20]. https://medium.com/coinmonks/cross-chain-technology-the-future-of-blockchain-interoperability-145f808cf426.

[3] YANG G Z,ZANG C,CHEN J J,et al.Distributed fusion cross-chain model and architecture[J]. IET Blockchain, 2022,2(2):29-43.

[4] Institute of Electrical and Electronics Engineers.IEEE standard computer dictionary:A compilation of IEEE standard computer glossaries[M].New York. NY,1990.

[5] Trusted blockchain to advance plans. Blockchain Interoperability White Paper[R/OL]. (2020-07-01) [2022-09-28].http://www.trustedblockchain.cn/.
可信区块链推进计划.区块链互操作白皮书[R/OL]. (2020-07-01) [2022-09-28]. http://www.trustedblockchain.cn/.

[6] NICK W.A Fork in the Blockchain: Income Tax and the Bitcoin/Bitcoin Cash Hard Fork[EB/OL].(2018-05-01) [2022-09-19].https://scholarship.law.unc.edu/ncjolt/vol19/iss4/10.

[7] SILVA F J C,DAMSGAARD S B,SORENSEN M A M,et al.Analysis of Blockchain Forking on an Ethereum Network[C]//European Wireless 2019; 25th European Wireless Conference, Aarhus, Denmark ,May 02-04, 2019. Piscataway: IEEE,2019:1-6.

[8] WANG G,SHI Z J,NIXON M,et al.SoK: Sharding on Blockchain[EB/OL]. [2022-09-26]. https://eprint.iacr.org/2019/ 1178.pdf.

[9] github.ethereum/wiki.Sharding FAQs[EB/OL].(2022-05-24) [2022-10-05].https://github.com/ethereum/wiki/wiki/ Sharding-FAQs.

[10] JANG N Q,BAI F H,HUANG L,et al.Reputation-Driven Dynamic Node Consensus and Reliability Sharding Model in IoT Blockchain[J].Algorithms,2022,15(2):1-22.

[11] LI X Q,JIANG P,CHEN T,et al.A survey on the security of blockchain systems[J].Future Generation Computer Systems, 2020,107(06):841-853.

[12] HOPE-BAILIE A,THOMAS S.Interledger: Creating a Standard for Payments[C]//Proceedings of the 25th International Conference Companion on World Wide

Web,Montréal Québec,Canada,April 11-15,2016.New York: ACM,2016:281-282.
[13] NOLAN T.Alt chains and atomic transfers[EB/OL]. (2013-05-01)[2022-03-15].https://bitcointalk.org/index.php?topic=193281.0.
[14] HERLIHY M.Atomic Cross-Chain Swaps[J].Computer Science>Distributed,Parallel,and Cluster Computing,arXiv: 1801.09515v4,2018.
[15] BACK A,CORALLO M,DASHJR L,et al.Enabling Blockchain Innovations with Pegged Sidechains[EB/OL]. (2014-10-22)[2022-03-16].https://www.blockstream.com/sidechains.pdf.
[16] POON J,DRYJA T.The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments[EB/OL]. (2016-01-14)[2022-03-16].https://lightning.network/lightning-network-paper.pdf.
[17] ConsenSys.Welcome to BTC Relay's documentation![EB/OL].[2022-03-18].https://btc-relay.readthedocs.io/en/latest/.
[18] KWON J,BUCHMAN E.A Network of Distributed Ledgers[EB/OL].[2022-03-18].https://v1.cosmos.network/resources/whitepaper.
[19] WOOD G.Polkadot:Vision for a heterogeneous multi-chain framework(draft1)[EB/OL]. (2016-11-10) [2022-03-22]. https://polk- adot.network/Polkadot-lightpaper.pdf.
[20] Ethereum Wiki.On sharding blockchains FAQs[EB/OL].[2020-03-26].https://eth.wiki/sharding/Sharding-FAQs.
[21] EYKHOLT E,MEREDITH L G,DENMAN J.RChain Architecture Documentation Release 0.8.1[EB/OL]. (2017-01-12)[2022-03-28].https://github.com/rchain/reference/blob/master/docs/RChainWhitepaper.pdf.
[22] Overline Team.Overline Whitepaper[EB/OL].(2021-06-05) [2022-03-28].https://overline.network/whitepaper.pdf.
[23] SPOKE M,Nuco Engineering Team.Aion:The third-generation blockchain network[EB/OL].(2017-07-31) [2022-03-30].https://aion.network/downloads/aion.network_technical-introduction _zh.pdf.
[24] POON J,BUTERIN V.Plasma:Scalable Autonomous Smart Contracts[EB/OL].(2017-08-11)[2020-03-31].https:// plasma.io/plasma.pdf.
[25] BUTERIN V.Minimal Viable Plasma[EB/OL]. (2018-01-03)[2022-04-06].https://ethresear.ch/t/minimal-viable-plasma/426.
[26] BUTERIN V.Plasma Cash: Plasma with much less per-user data checking[EB/OL].(2018-03-04)[2022-04-06]. https://ethresear.ch/t/plasma-cash-plasma-with-much-less-per-user-data-checking/1298.
[27] Robinson D.Plasma Debit: Arbitrary-denomination payments in Plasma Cash[EB/OL].(2018-06-11) [2022- 04-06]. https://ethresear.ch/t/plasma-debit-arbitrary-denomi- nation-payments-in-plasma-cash/2198.
[28] JONES B,FICHTER K.More Viable Plasma[EB/OL].(2018-06-07)[2022-04-07].https://ethresear.ch/t/more-viable-plasma/2160.
[29] Wormhole.Wormhole: A Smart Contract Solution for Bitcoin Cash[EB/OL].(2018-007-15)[2020-04-03].https://wormhole.cash/whcwhitepaper-en.pdf.
[30] LI DAWEI,LIU JIANWEI,TANG ZONGXUN,et al. AgentChain:A Decentralized Cross-Chain Exchange System[C]//2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, Rotorua, New Zealand, Aug 5-8, 2019. Piscataway: IEEE,2019:491-498.
[31] PUPYSHEV A,GUBANOV D,DZHAFAROV E,et al. Gravity: a blockchain-agnostic cross-chain communication and data oracles protocol[J]. Computer Science> Cryptography and Security,arXiv:2007.00966,2020.
[32] LAN R,UPADHYAYA G,TSE S,et al.Horizon:A Gas- Efficient, Trustless Bridge for Cross-Chain Transac- tions[J]. Computer Science>Cryptography and Security, arXiv: 2101.06000,2021.
[33] WESTERKAMP M,DIEZ M.Verilay: A Verifiable Proof of Stake Chain Relay[J].Computer Science>Cryptography and Security,arXiv:2201.08697,2022.
[34] HEI Y M,LI D W,ZHANG C,et al.Practical AgentChain: A compatible cross-chain exchange system[J]. Future Generation Computer Systems,2022,130:207-217.
[35] XU C C,WANG X Y,XIA L W,et al.BitXHub WHITEPAPER[EB/OL].(2022-07-01)[2022-10-30].https://upload.hyperchain.cn/BitXHub%20Whitepaper.pdf.
[36] WeBank/WeCross[EB/OL].[2022-10-30].https://gitee.com/WeBank/WeCross.
[37] BRUDGES J ,CEVALLOS A,CZABAN P,et al.Overview of Polkadot and its Design Considerations[J].Computer Science>Cryptography and Security, arXiv:2005.13456v3, 2020
[38] BUTERIN V.Chain Interoerability[EB/OL]. (2016- 09-09) [2022-11-05].https://www.r3.com/reports/chain-interoperability/.
[39] TREAT D,SCHIATTI L,GIORDANO G,et al.Connecting ecosystems: Blockchain integration[EB/OL].(2018-10-22) [2022-11-05].https://www.01caijing.com/viewer/pdf.htm?filePath=attachment/202003/C490A9355914412.pdf.
[40] World Economic Forum.Inclusive Deployment of Blockchain for Supply Chains:Part 6 – A Framework for Blockchain Interoperability(White Paper)[EB/OL]. (2020- 04-04) [2022-11-05].https://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf.
[41] LESAVRE L,VARIN P,YAGA D.Blockchain Networks:Token Design and Management Overview[EB/OL].(2021-02-01)[2022-02-01].https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8301.pdf.
[42] FUSION Foundation.Distributed Control Rights Management Signature Verification Program[EB/OL]. [2022-11-09].https://github.com/FUSIONFoundation/dcrm/.
[43] GAŽI P,KIAYIAS A, ZINDROS D. Proof-of-Stake Sidechains[C]//2019 IEEE Symposium on Security and Privacy (SP),San Francisco,CA,USA.May 19-23,2019. Piscataway:IEEE,2019:139-156.
[44] aelf Developer.aelf Tech Talks-Cross-Chain Mechanism Breakdown[EB/OL].(2020-05-19)[2022-11-06].https://medium.com/aelfblockchain/tagged/chain-interoperability.
[45] BACK A,CORALLO M,DASHJR L,et al.Enabling blockchain innovations with pegged sidechains[EB/OL]. (2014-10-22)[2022-11-06].https://docs.huihoo.com/blockstream/sidechains.pdf.
[46] FRAUENTHALER P,SIGWART M,SPANRING C,et al. Testimonium:A Cost-Efficient Blockchain Relay[J]. Computer Science>Cryptography and Security,arXiv:2002.12837,2020.
[47] MENG B,WANG Y B,ZHAO C,et al. Survey on Cross-Chain Protocols of Blockchain[J].Journal of Frontiers of Computer Science and Technology, 2022,

16(10):2177-2192.
孟博,王乙丙,赵璨,等.区块链跨链协议综述[J].计算机科学与探索,2022,16(10):2177-2192.
[48] WANG W.Simplified Payment Verification:Instant payment, signature validity, and the importance of integrity[EB/OL].(2020-08-25)[2022-11-06].https://medium.com/nchain/simplified-payment-verification-48ac60f1b26c.
[49] DAI B R,JIANG S M,ZHU M L,et al.Research and Implementation of Cross-Chain Transaction Model Based on Improved Hash-Locking[C]//Second International Conference,BlockSys 2020, Dali,China,August 6–7, 2020. Berlin, Heidelberg:Springer,2020:218-230.
[50] European Central Bank.Synchronised cross-border payments[EB/OL].(2019-06-01)[2022-11-09].https://www.boj.or.jp/en/announcements/release_2019/data/rel190604a1.pdf.
[51] GRAHAM D A.Sequential Games[EB/OL].(2007-06-18)[2022-11-10].https://people.duke.edu/~dgraham/ECO_463/Handouts/SequentialGames.pdf.
[52] KATE A,GOLDBERG I.Distributed Private-Key Generators for Identity-Based Cryptography[C]//SCN 2010: Security and Cryptography for Networks,Amalfi,Italy, September 13-15, 2010. Berlin, Heidelberg:Springer,2010:436-453.
[53] LOUIE T.Welcome to Wanchain[EB/OL].(2021-04-23)[2022-11-13].https://medium.com/wanchain-foundation/an-introduction-to-wanchain-a2936e25df91.
[54]GOES C.The Interblockchain Communication Protocol: An Overview[J].Computer Science>Distributed,Parallel, and Cluster Computing,arXiv:2006.15918,2020.
[55] W3F(Web3 Foundation).XCMP overview[EB/OL].[2023-02-17].https://research.web3.foundation/en/latest/polkadot/XCMP/index.html.
[56] WANG H K,HE D,GAO Y,et al.Research on Data Verification and Exchange of Heterogeneous Blockchains for Electricity Application[C]//2nd International Con- ference on Artificial Intelligence and Computer Science,Hangzhou, Zhejiang,China,July 25-26,2020.IOP Publishing,2020,1631:1-6.
[57] Chainlink. Cross-Chain Interoperability Protocol (CCIP)[EB/OL].[2023-02-18].https://chain.link/cross-chain#cross-chain-interoperability-protocol.
[58] KALEEM M,SHI W.Demystifying Pythia: A Survey of ChainLink Oracles Usage on Ethereum[J].Computer Science>Distributed, Parallel, and Cluster Computing, arXiv:2101.06781v2,2021.
[59] BREIDENBACH L,CACHIN C,CHAN B,et al.Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks[EB/OL].(2021-04-15)[2023-02-17].https:// research.chain.link/whitepaper-v2.pdf?_ga=2.119185609.1361700968.1676778827-249784990.1676778827.
[60] ZARICK R,PELLEGRINO,B,BANISTER C.LayerZero: Trustless Omnichain Interoperability Protocol[J].Computer Science>Networking and Internet Architecture, arXiv: 2110.13871v1,2021.
[61] ADLER J,BERRYHILL R,BENERIS A,et al.Astraea: A Decentralized Blockchain Oracle[J].Help | Advanced Search, Computer Science>Cryptography and Security, arXiv:1808.00528,2018.
[62] LERNER S D.Rootstock platform,bitcoin powered smart contracts[EB/OL].(2020-05-06)[2022-11-12].http:// cryptochainuni.com/wp-content/uploads/Rootstock-WhitePaper-v9-Overview.pdf.
[63] SIRIS V A,NIKANDER P,VOULGARIS S,et al. Interledger Approaches[J]. IEEE Access, 2019, 7:89948-89966.
[64] THOMAS S,SCHWARTZ E.A Protocol for Interledger Payments[EB/OL]. (2015-01-01) [2022-11-16]. https:// interledger.org/interledger.pdf.
[65] HYPERCHAIN.BitXHub White Paper V2.0- Blockchain cross-chain technology platform[EB/OL].(2022-07-01)[2022-11-20].https://upload.hyperchain.cn/BitXHub%E7%99%BD%E7%9A%AE%E4%B9%A6.pdf.
趣链科技.BitXHub 白皮书 V2.0-区块链跨链技术平台[EB/OL].(2022-07-01)[2022-11-20].https://upload.hyperchain.cn/BitXHub%E7%99%BD%E7%9A%AE%E4%B9%A6.pdf.
[66] YE S J,WANG XY,XU C C,et al.BitXHub:Dide-relay Chain Based Heterogeneous Blockchain Interoperable Platform[J].Computer Science,2020,47(06):294-302.
叶少杰,汪小益,徐才巢,等.BitXHub:基于侧链中继的异构区块链互操作平台[J].计算机科学,2020,47(06):294-302.
[67] PAPADIS N,TASSIULAS L.Blockchain-Based Payment Channel Networks: Challenges and Recent Advances[J]. IEEE Access,2020,8:227596-227609.
[68] DECKER C,WATTENHOFER R. A fast and scalable payment network with bitcoin duplex micropayment channels[J]. Symposium on Self-Stabilizing Systems, 2015:3-18.
[69] CHEN Y J ,ZHU X T,YU Y R,et al.Empirical Analysis of Lightning Network: Topology, Evolution, and Fees[J]. Journal of Software,2022,33(10):3858-3873 .
陈艳姣,朱笑天,于永瑞,等.区块链闪电网络实证分析:拓扑、发展和收费策略[J].软件学报,2022,33(10):3858-3873.
[70] LU J,YANG B,LIANG Z.et al.Building Super Financial Markets for the New Digital Economy WANCHAIN Whitepaper Version 0.9.1[EB/OL].(2017-01-01) [2022-12-03].https://www.wanchain.org/_files/ugd/9296c5_0d623032c67b4e2380e14452ec02a9e4.pdf.
[71] Wanchain.Cross-Chain Overview[EB/OL].[2022-12-02].https://docs.wanchain.org/technology/cross-chain-overview.
[72] GUO D,SHI C,CHEN Y.Galaxy Consensus: A Practical Proof-of-Stake Protocol With a Robust Delegation Mechanism[EB/OL].https://www.wanchain.org/_files/ugd/9296c5_5205d584ee594e879d4b8b58048b6fac.pdf.
[73] MECHANIC Q.Proof of stake[EB/OL].(2011-07-11)[2022-12-05].https://bitcointalk.org/index.php?topic=27787.
[74] SASAKI Y,WANG L,AOKI K.Preimage Attacks on 41-Step SHA-256 and 46-Step SHA-512[EB/OL]. [2022-12-16].https://eprint.iacr.org/2009/479.pdf.
[75] ROHRER E,MALLIARIS J,TSCHORSCH F.Discharged Payment Channels: Quantifying the Lightning Network's Resilience to Topology-Based Attacks[J].Computer Science>Networking and Internet Architecture, arXiv:1904.10253,2019.
[76] MARTINAZZI S,FLORI A.The evolving topology of the

Lightning Network: Centralization, efficiency, robustness, synchronization, and anonymity[J],Public Library of Science,2020,15(1):1-18.
[77] KIM H M,LASKOWSKI M.Toward an ontology-driven blockchain design for supply-chain provenance[J]. Intelligent Systems in Accounting,Finance and Management, 2018,25(1):18-27.
[78] HARVEY C R.The DAO[EB/OL].[2023-02-20].https://people.duke.edu/~charvey/Teaching/697_2019/ Presentations/DAO.pdf.
[79] YAGA D,MELL P,ROBY N,et al.Blockchain Technology Overview[EB/OL].(2018-10-01)[2022-12-16].https://doi.org/10.6028/NIST.IR.8202.
[80] DASGUPTA D,SHREIN J M,GUPTA K D.A survey of blockchain from security perspective[J]. Journal of Banking and Financial Technology,2019,3(1):1-17.
[81] WEILER N.Honeypots for Distributed Denial of Service Attacks[EB/OL].[2022-102-20].http://www.csl.mtu.edu/ cs6461/www/Reading/Weiler02.pdf.
[82] WUST K,GERVAIS A.Ethereum Eclipse Attacks[EB/OL].(2016-01-01)[2022-12-20].https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/121310/eth-49728-01.pdf.
[83] BUTERIN V.Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform[EB/OL].(2014-12-01)[2022-12-20].https://courses.cs.duke.edu/spring23/compsci512/papers/ethereum.pdf.
[84] YAFFE L.Investigating Long Range Attack[EB/OL].(2018-12-11)[2022-12-21].https://medium.com/hackernoon/investigating-long-range-attack-2bce0887a2da.
[85] FANTI G,KOGAN L,OH S,et al.Compounding of Wealth in Proof-of-Stake Cryptocurrencies[J].Computer Science> Cryptography and Security,arXiv:1809.07468,2018.
[86] MIT Media lab.51% attacks[EB/OL].[2022-12-20].https://dci.mit.edu/51-attacks.
[87] ROBERTO J.Understanding Proof of Stake: The Nothing at Stake Theory[EB/OL].(2018-06-08)[2022-12-21].https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027.
[88] JOHN A.On Public Crowdsource-Based Mechanisms for a Decentralized Blockchain Oracle[J].IEEE transactions on engineering management,2020,67(4);1444-1458.
[89] HE Y C,ZHU X Y,XU F F,et al.A Novel Cross-Chain Mechanism for Blockchains[C]//First International Conference, SmartBlock 2018,Tokyo,Japan,December 10-12, 2018.Berlin,Heidelberg:Springer,2018:139-148.

王群（1971-），男,甘肃天水人，博士，现为江苏警官学院教授，CCF 会员,主要研究领域为信息安全,计算机网络体系结构与协议。

WANG Qun was born in 1971. He received the Ph.D. degree from Nanjing University of Science and Technology in 2016. He is a professor at Jiangsu Police Institute, and the member of CCF. His research interests include information security, computer network architecture and protocols, ETH.

李馥娟（1974-），女，陕西西安人，硕士，现为江苏警官学院教授，主要研究领域为计算机网络技术与应用，信息安全。

LI Fujuan was born in 1974. She is a professor at Jiangsu Police Institute. Her research interests include computer network technology and application, information security, ETH.

倪雪莉（1990-），女，江苏南通人，2016 年于南京信息工程大学获得硕士学位，现为江苏警官学院讲师，主要研究领域为电子数据取证、网络空间安全。

NI Xueli(1990-), born in Nantong, Jiangsu, she obtained her Master degree from Nanjing University of Information Technology in 2016. She is currently a lecturer at Jiangsu Police Institute. Her main research areas are digital forensics and cyberspace security, ETH.

夏玲玲（1988-），女，江苏射阳人，2017 年于南京邮电大学获得博士学位，现为江苏警官学院副教授，江苏省网络空间安全学会会员，主要研究领域为网络安全，复杂网络传播动力学，网络爬虫和数据挖掘。

XIA Ling-Ling was born in 1988. She received the Ph.D. degree from Nanjing University of Posts and Telecommunications in 2017. She is an associate professor at Jiangsu Police Institute and the member of Jiangsu cyberspace security association. Her research interests include network security technology, spreading dynamics of complex networks, web crawler technology and data mining.

梁广俊（1982-），男，安徽芜湖人，2018 年于南京邮电大学获得博士学位，现为江苏警官学院副教授，主要研究领域为电子数据取证、网络空间安全。

LIANG Guangjun(1982-), born in Wuhu, Anhui, he obtained his Ph.D. degree from Nanjing University of Posts and Telecommunications in 2018. He is an associate professor at Jiangsu Police Institute. His main research areas are digital forensics and cyberspace security, ETH.

马卓（1993-），女，山西太原人，2021 年于东南大学获得博士学位，现为江苏警官学院讲师，主要研究领域为网络空间安全。

MA Zhuo (1993-), born in Taiyuan, Shanxi. She obtained her Ph.D. degree from Southeast University in 2021. She is currently a lecturer at Jiangsu Police Institute. Her main research area is cyberspace security.