计算机科学与探索
Journal of Frontiers of Computer Science and Technology
1673-9418/2022/16(10)-2177-16
doi: 10.3778/j.issn.1673-9418.2203032

区块链跨链协议综述

孟　博+,王乙丙,赵　璨,王德军,麻斌豪
中南民族大学 计算机科学学院,武汉 430074
+ 通信作者 E-mail: mengscuec@gmail.com

摘　要:随着区块链技术的发展,各区块链平台在系统架构、应用场景上有所不同,造成了不同区块链上的数据和资产难以互联互通,影响了区块链的推广与应用。跨链技术为解决区块链异构互联互通问题,提升区块链的互操作性和可扩展性提供了技术方案。而跨链协议是通过跨链技术实现不同区块链之间的跨链互操作性的具体设计规范,其对实现区块链互操作性和构建区块链跨链应用具有重要意义。对区块链跨链协议的最新研究进行了系统的整理和分析。从以下四方面进行介绍:首先,从链联网、跨链技术和区块链互操作性三方面阐述区块链跨链互操作的研究现状;其次,将跨链协议总结概括为跨链通信协议、跨链资产交易协议和跨链智能合约调用协议,并具体分析其最新研究进展;然后,对跨链协议的关键设计原则进行总结概括,为跨链协议的安全性、隐私性、可扩展性等问题提供解决思路;最后,结合区块链跨链应用的实际需求,给出区块链跨链协议未来的重点研究方向。

关键词:区块链;跨链互操作;跨链技术;跨链协议;跨链应用
文献标志码:A　　**中图分类号:**TP39;TP309.2

Survey on Cross-Chain Protocols of Blockchain

MENG Bo+, WANG Yibing, ZHAO Can, WANG Dejun, MA Binhao
College of Computer Science, South-Central Minzu University, Wuhan 430074, China

Abstract: With the development of blockchain technology, due to the different system architecture and application scenarios of blockchain platforms, it is difficult to realize the interconnection and intercommunication of data and assets on different blockchains, which affects the promotion and application of blockchain. The cross-chain technology of blockchain is an important technical solution to realize the interconnection of blockchain and improve the interoperability and extensibility of blockchain. The blockchain cross-chain protocol is the specific design specifications to realize the cross-chain interoperability between different blockchains through cross-chain technology, so it is of great significance to the realization of blockchain interoperability and the construction of blockchain cross-chain application. This paper systematically arranges and analyzes the latest researches on the integration and implementation of blockchain cross-chain protocols, and places them in four hierarchies: Firstly, the current research status of blockchain cross-chain interoperability is explained from three aspects, Internet of blockchains, cross-chain technology and blockchain interoperability. Secondly, the cross-chain protocols are divided into cross-chain communication agreements, cross-chain asset transaction agreements and cross-chain smart contract call agreements, and the

基金项目:国家重点研发计划(2020YFC1522900);湖北省自然科学基金(2018ADC150);中央高校基本科研业务费专项资金(CZZ21001,QSZ17007)。
This work was supported by the National Key Research and Development Program of China (2020YFC1522900), the Natural Science Foundation of Hubei Province (2018ADC150), and the Fundamental Research Funds for the Central Universities of China (CZZ21001, QSZ17007).
收稿日期:2022-03-07　　**修回日期:**2022-04-27

latest research is analyzed. Thirdly, the key design principles of cross-chain protocols are summarized, and the solutions for the problems of security, privacy and scalability of cross-chain protocol are provided. Finally, combined with the actual needs of blockchain cross-chain applications, the future research direction of blockchain cross-chain protocol is given.

Key words: blockchain; cross-chain interoperability; cross-chain technology; cross-chain protocol; cross-chain application

区块链是一种分布式账本技术,其具备过程可信和去中心化两大特性,能够在多利益主体参与的场景下以低成本的方式构建信任,可以重塑社会信用体系[1]。随着区块链技术的快速发展,区块链技术应用日益广泛,已经在金融、电子政务、车联网、数字身份、版权保护等多个领域得到广泛应用[2-4]。目前,区块链加速构建新一代的价值网络和契约社会,其最大意义在于链接不同行业,解决信任难题,实现数据和资产的可信流转,进一步提高生产效率,从而激发经济增长动力。

区块链技术发展至今,经历了以比特币技术为代表的区块链1.0阶段和以智能合约技术和联盟链为代表的区块链2.0阶段,目前区块链进入了以各行业的区块链应用融合为代表的区块链3.0阶段[5]。在区块链1.0阶段中,区块链技术围绕数字资产的发行和交易进行架构设计,在金融领域初步应用。在区块链2.0阶段中,随着智能合约技术的发展,区块链在金融领域得到更加广泛的应用,也开始扩展使用到其他行业。而在区块链3.0阶段中,随着区块链技术的逐渐成熟,区块链开始应用到金融、经济、科技和政务等领域,面临更加复杂的业务需求,开始产生跨异构链进行数据、资产和功能的互联互通需求,并向跨链应用发展。但是不同区块链系统之间在互联互通上的欠缺,极大限制和阻碍了区块链技术的进一步发展与应用。

随着跨链技术的发展,解决跨链难题的技术方案不断涌现,在区块链跨链领域中诸多学者对跨链技术进行整理总结,分析主流跨链技术的特点和挑战。其中,李芳等人[6]从跨链技术的原理与实现思路出发,分析跨链技术的安全风险;徐卓嫣等人[7]从跨链技术的主要挑战出发,对比主流跨链解决方案;路爱同等人[8]从跨链技术难点出发对主流跨链技术进行分析。以上学者着重关注跨链技术,较少关注跨链协议。在区块链跨链领域中,跨链技术提供了技术解决思路,而跨链协议则是具体的设计规范,设计实现跨链互操作的同时对安全性、可扩展性、隐私性等方面进行设计,为跨链应用提供解决方案。因此跨链协议是实现区块链跨链互操作和构造跨链应用的关键和基础。随着区块链跨链领域向着跨链应用方向不断发展,有必要对跨链协议的最新研究成果进行全面的总结与分析。

1 链联网与跨链

1.1 链联网定义

随着区块链技术的蓬勃发展,从公有链到联盟链,从数字货币到产业应用,区块链应用领域不断扩大,区块链技术走向生产实践,链与链之间的应用与数据的互联互通需求成为区块链发展道路上迫切需要解决的难题。2018年,Vo等人[9]首次提出链联网的概念,并设想链联网未来的发展方向。链联网(Internet of blockchains, IoB)指同构或异构区块链之间形成一个互相通信的去中心化网络,以促进价值、数据和状态转换的跨链交易。从技术角度看,链联网的实现涉及跨链技术、智能合约、区块链预言机等技术。从应用角度看,链联网旨在实现不同链的价值、数据和功能互通,进而实现跨链应用,推动区块链技术的进一步发展。从网络空间安全角度看,链联网涉及去中心化区块链网络中的数据可信验证、数据隐私保密等核心安全性要求。

1.2 跨链技术

目前,已有公证人机制(notary scheme)[10]、哈希锁定(hash-locking)[11]、侧链(sidechain)[12]、中继(relay)[13]和分布式私钥控制(distributed private key control)[14]这五种主流跨链技术,在不同程度上解决了跨链互操作问题,为实现跨链提供了技术方案。

公证人机制通过引入第三方来验证交易信息是否一致、合法,无需对交易的细节进行验证。其优点是实现原理简单且无需复杂工作量证明,缺点是有中心化风险。公证人机制主要包括三种类型:单签公证人、多重签名公证人、分布式签名公证人。单签公证人又称中心化公证人机制,其通过单一的独立节点或机构充当公证人角色。多重签名公证人通过

多个公证人进行签名的方式提高公证人机制的安全性。分布式签名公证人采用多方计算（multi-party computation，MPC）实现安全性。

哈希锁定机制又称为哈希时间锁定协议（hashed-timelock agreements，HTLA），是一种基于原子交换的跨链机制，其通过资产锁定并设置相应的时间和解锁条件来实现资产交换，并实现原子性。优点是安全性高，缺点是使用场景有限。哈希锁定机制只支持资产或者信息交换，而不支持资产或者信息转移。

侧链又称为锚定侧链（pegged sidechains），是一种通过双向挂钩（two-way peg）实现在不同区块链之间转移资产或数据信息的跨链技术。其中，双向挂钩是侧链机制实现的核心。侧链的缺点在于网络和资产的复杂度增加，新攻击媒介的产生和中心化挖矿的风险[15]。

中继机制不完全依赖于可信第三方的验证判断，仅通过中间人收集不同链的数据状态进行自我验证。在中继机制中，平行链通过遵守协议规范与中继链连接，当平行链需要发起跨链操作时，平行链需要将跨链互操作的交易信息通过中继链的验证者审核后发布到中继链上，由中继链传递信息到目标平行链上实现跨链互操作。

侧链机制和中继机制的优点在于扩展性、安全性有一定保证，且使用场景广泛，而缺点是侧链实现难度较大。侧链机制和中继机制的区别在于：中继通过中间链的方式实现不同链之间数据状态的验证，而侧链是通过双向锚定实现性能拓展的解决方案。

分布式私钥控制是使用分布式私钥的生成与控制来实现将多种不同区块链的数字资产映射到一条新的区块链上，并在这条新的区块链上实现不同链之间的数字资产交换。分布式私钥控制技术基于分布式的密钥分发机制，类似分布式签名公证人，但其进一步避免中心化风险。分布式私钥控制技术目前的使用场景有限，只应用于数字资产领域。

对主流跨链技术的分析与比较如表1所示。从对比结果看：在安全性方面，目前主流跨链技术的安全性有待进一步加强；在应用场景方面，哈希锁定的应用场景比较有限，仅仅支持实现资产的跨链交换。总之，目前同一应用场景下可采用多种跨链技术，此时需要将跨链技术的原理与应用背景结合，选择最合适的跨链技术去解决实际应用问题。

1.3　区块链互操作性

一般来说，互操作性指不同系统和组织机构之间协同工作的能力。在计算机科学领域，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。Wegner[16]指出互操作性是不同语言、接口和执行平台的软件组件之间的合作能力。Vernadat[17]认为企业系统之间的互操作性为衡量软件、流程、系统、业务单元这些实体之间的互操作能力，关键是如何促进这些实体的沟通、合作和协调。区块链互操作性主要是指不同区块链之间通过跨链技术手段实现互联互通。

关于区块链互操作性，不同学者进行了总结归纳。Koens等人[18]概括将区块链互操作性分为三类：第一类是区块链系统与现存系统的互操作性；第二类是不同区块链间的互操作性；第三类是单独的区块链上不同智能合约之间的互操作性。以上概括缺少对区块链互操作性实际功能的关注。Buterin[19]认为区域链互操作性是两个区块链之间通过引入第三方，并在不改变原生链的情况下进行跨链的资产转移、支付或者信息交互的能力。Jin等[20]提出区块链互操作性是从一条区块链到另一条区块链的有效通信和直接信息交换的特性，同时保留了每个区块链

表1　跨链技术对比分析

Table 1　Comparison and analysis between cross-chain technology

比较维度	公证人[10]	哈希锁定[11]	侧链[12]/中继[13]	分布式私钥控制[14]
安全性	低	中	低	中
交易速度	慢	中	慢	中
可扩展性	较强	有限	强	有限
智能合约支持程度	困难	不支持	困难	困难
应用场景	全部	有限	全部	全部
实现难度	容易	容易	中等	中等
局限性	依赖第三方公证人	应用场景单一	交易速度慢	智能合约功能有待完善
实现原理	信任一组公证人	验证哈希锁和时间锁	采集原链信息进行验证	分离资产的所有权和使用权
典型项目	Interledger/Croda	Lightning Network	Cosmo/Polkadot	Wanchain/Fusion

表2 跨链互操作性概念对比

Table 2 Concept comparison between cross-chain interoperability

年份	提出者	核心观点	关注点
2016	Buterin[19]	通过引入第三方,并在不改变原生链的情况下进行跨链的互操作	跨链技术
2018	Jin等人[20]	链与链之间的有效通信和直接信息交换	数据互通
2019	Abebe等人[21]	不同区块链之间传输或交换数据或价值	数据互通;价值互通
2019	Borkowski等人[22]	跨链数据转移、跨链智能合约调用和跨链资产转移	数据互通;价值互通;功能互通
2019	Schulte等人[23]	跨链资产转移和跨链智能合约调用	价值互通;功能互通
2020	Belchior等人[24]	源区块链进行跨链,改变目标区块链的状态	跨链技术
2020	Kannengießer等人[25]	从外部系统检索数据或与外部系统交换数据	数据互通
2020	Lafourcade[26]	创建包含两个分布式账本的二合一区块链	数据互通
2020	叶少杰等人[27]	进行资产交易、信息互通、服务互补等跨链功能	数据互通;价值互通;功能互通

的本质,包括不可逆性和可追溯性。Abebe等[21]将区块链互操作性定义为不同分布式账本之间的语义依赖,目的是传输或交换数据或价值,并保证有效性或可验证性。对区块链互操作性的观点总结如表2所示。

根据对以上区块链互操作性概念的分析和总结,认为区块链互操作性,又称跨链互操作性,主要表现为数据互通、价值互通与功能互通。数据互通关注不同区块链之间的跨链数据访问与跨链数据传递。价值互通关注不同区块链之间的跨链资产互换与跨链资产转移。功能互通旨在实现不同区块链之间功能融合,如实现跨链调用智能合约。因此跨链协议主要包含跨链通信协议、跨链资产交易协议和跨链智能合约调用协议。跨链协议是实现链联网和区块链跨链互操作的关键和基础。其中,跨链通信协议实现数据互通,跨链资产交易协议实现价值互通,跨链智能合约调用协议实现功能互通。区块链互操作性如图1。

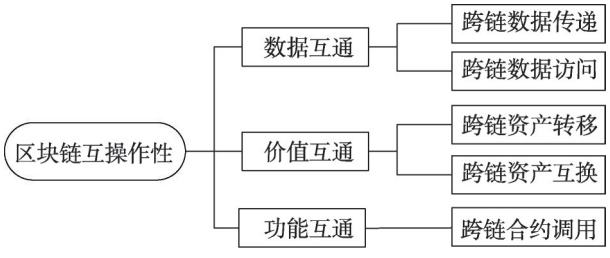


图1 区块链互操作性

Fig.1 Blockchain interoperability

2 跨链协议

跨链协议依托于跨链技术,通过定义一系列通信数据格式、协议规范、共识协议等,实现区块链跨链互操作。Zamyatin等人[28]定义跨链通信协议的有效性、原子性和及时性等概念,介绍基于跨链通信协议实现跨链通信。Belchior等人[24]定义跨链通信协议为实现同构区块链或异构区块链间的通信交互,并达成跨链事务同步的过程。自基于哈希锁定的原子交换技术[29]应用于区块链实现跨链数字资产交换后,学术界开始基于原子交换、侧链、中继等跨链技术设计跨链资产交换协议以实现跨链资产互换。Schulte等人[23]指出为解决链上数字资产只能在原链上使用的局限性问题,需设计跨链资产转移协议,从而建立在不同区块链上转移数字资产的方法。其中,跨链资产交换协议和跨链资产转移协议两者对象都是链上的数字资产,因此将两者总结归纳为跨链资产交易协议。Nissl等人[30]提出跨链智能合约调用的概念,强调通过实现跨区块链的智能合约调用,进而实现跨区块链的互操作性,引出跨链智能合约调用协议。综合上述研究,可将跨链协议总结为跨链通信协议、跨链资产交易协议和跨链智能合约调用协议三类。具体而言,跨链通信协议通过跨链数据通信实现数据互通,跨链资产交易协议通过跨链资产交易实现价值互通。跨链智能合约调用协议通过跨链智能合约调用实现功能互通。

2.1 跨链通信协议

跨链通信协议通过传输、读取和验证其他链或链外的状态或事件,实现数据的传递与访问。当前主要的跨链通信协议有IBC(interblockchain communication protocol)[31]、MBCCP(multi-blockchain consociation and communication protocol)[32]、XCMP(cross-chain message passing)[33]和IBTP(interblockchain transfer protocol)[34]。

IBC协议[31]由Goes提出,应用于Cosmos平台,是一种端到端、面向连接、有状态的协议,具备消息验证、多路复用、超时处理等功能。IBC协议实现基于中继的跨链通信,由客户端、连接、通道、中继器组

成。客户端负责验证跨链交易的轻客户端,确保执行交易的有效性和合法性。连接是基于轻客户端建立握手连接,通过发送和接收特定数据包的形式判断连接是否成功。通道基于应用层实现数据包传输,实现跨链交易的有序性,并确保数据包只发送一次,通过一个连接与多个通道匹配的方式来提供多路复用功能。中继器负责在运行IBC协议的多个分布式账本系统之间传递数据。在安全性方面,应用共识算法的最终性(finality)来防止双花。Tendermint和PBFT(practical Byzantine fault tolerance)类共识算法满足Cosmos的最终性要求,而PoW(proof of work)、PoS(proof of stake)、DPoS(delegated proof of stake)类的概率共识算法提供概率最终性,需要应用层选择安全阈值。

MBCCP协议[32]由She等人提出,应用于跨链通道匹配模型。该协议原理如图2所示。MBCCP协议通过在不同区块链间创建对等节点匹配通道实现可信跨链信息传输,应用PM共识机制实现参与链的节点管理和匹配问题。其跨链通信过程如下:首先由锚定中继链锚定参与链的主节点并创建相应的映射节点,同步原链的相关信息并提交给order节点。然后order节点选取参与链上的节点,并将节点信息广播给所有order节点,当某个节点收取到(3n+1) / 4个相同信息时达成共识并向其他所有节点广播,从而将该共识信息记录入区块链。order节点将选取的节点通过映射节点广播给所有参与链上的节点。最后PM共识机制完成,触发智能合约创建对等节点匹配通道,并将通过PM共识机制选取的节点加入到通道中,通过该通道完成跨链数据交换。

XCMP协议[33]由Burdges等人提出,应用于Polkadot平台,实现平行链之间的信息传输。XCMP允许双向通信的消息传递通道在平行链间传递数据。XCMP协议具备快速、有序性、可验证性、一致性、可用性和安全性。在有序性方面,通过输入/输出验证可确保跨链输出的消息保持正确的顺序。在可验证性方面,应用中继链状态来验证消息的来源与处理。中继链状态用平行链块头信息为平行链之间的区块提供了时间同步,进而在中继链中对发送的消息进行验证。在一致性方面,即使发生了链重组,接收到的消息也不会改变。在可用性方面,通过可用于重构消息的纠删码实现。在安全性方面,应用中继链实现共享安全性,另外基于SPREE(shared protected runtime execution enclaves)确保消息传递的正确性和可用性。

IBTP协议[34]由Wang等人提出,应用于BitXHub平台。IBTP协议以中继链作为跨链交易的合法性验证和交易路由平台,支持无状态的跨链消息转发,应用跨链网关实现多层级的跨链消息路由,构建高可扩展的、兼容性良好的区块链价值网络。IBTP协议通过数据包进行消息传递,规定了跨链消息的主要数据字段,旨在提供统一的跨链交易传输、路由和验证格式,保证跨链交易的有序性和跨链数据的可信验证,通过特殊序列化规则、DH(Diffie-Hellman)秘钥协商、隐私交易三种方法保护数据隐私。

此外,Wu等人[35]提出一种公平且有效的周期性委员会轮换协议,结合公证人机制和中继机制,提出

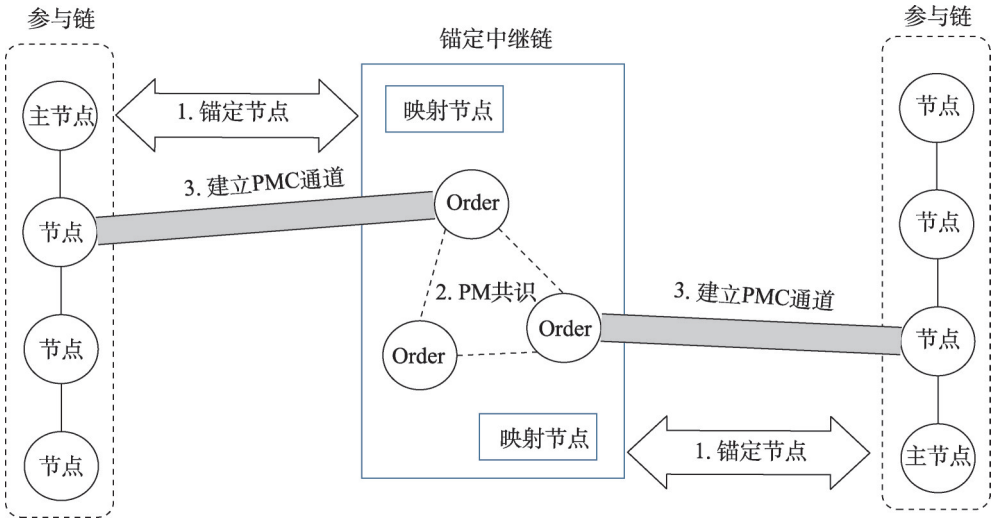


图2　MBCCP协议

Fig.2　MBCCP protocol

中继委员会机制，实现跨异构区块链的数据访问机制。Luo等人[36]基于三阶段事务提交协议提出支持原子性和一致性的跨链通信协议，规定路由消息的格式与消息传输流程，并设计了执行失败时的回滚操作和重传协议。康博涵等人[37]在Luo等人工作基础上，提出适用于智能服务交易的跨链通信服务协议，在满足三阶段事务提交协议的基础上支持原子性和一致性。

对典型跨链通信协议的跨链技术、可验证性、安全性、隐私性、可扩展性、跨链类型和局限性对比分析如表3所示。关于可验证性，大部分跨链通信协议基于现有的公证人机制或默克尔证明的SPV（simplified payment verification）验证机制实现数据验证，在一定程度上确保数据的真实性。关于安全性，现有跨链通信协议通过设计基于三阶段提交协议的分布式事务机制、基于交易日志的崩溃恢复机制、交易超时重传机制等确保跨链交易的安全性，但是未考虑到数据通信过程中对数据安全性的保护，比如如何确保数据的保密性。关于隐私性，现有的大部分跨链通信协议未考虑到数据通信过程中的隐私性，缺少对用户数据和交易数据的隐私保护。关于可扩展性，基于中继的跨链通信协议尽管可扩展性较高，但是依然存在部分跨链通信协议实现跨异构链通信的难度较大。

2.2 跨链资产交易协议

跨链资产互操作包含跨链资产转移和跨链资产交换。跨链资产交换（cross-chain asset swap）又名原子交换（atomic swap），是具备原子性和一致性的跨链交易，本质上是资产在各自区块链上的流动。如Alice和Bob在以太坊和比特币上都有账户，Alice想用20个以太币换取Bob的1个比特币，Alice需要先将自己账户的20个以太币转账给Bob在以太坊上的账户，Bob在收到付款后，将自己在比特币账户上的1个比特币转给Alice在比特币上的账户。跨链资产转移（cross-chain asset transfers）支持不同链之间的资产转移且支持原子性和去中心化一致性，其本质上是资产在一个区块链上的冻结（销毁）和在另一个区块链上的解冻（创建）。如Alice与Bob分别在比特币和以太坊上拥有账户，Alice想将自己的1个比特币转移给Bob，Alice需要先将她的比特币转移到一个特殊的地址进行冻结，然后在以太坊中发行（或解冻）20个以太币给Bob的账户（假设以太坊和比特币之间的汇率为20）。Herlihy等人[38]将跨链资产交换和跨链资产转移共同构成的跨链资产互操作总结为一种计算抽象，其反映标准商业实践活动中的商业互动，执行复杂的分布式状态变化。跨链资产交换协议和跨链资产转移协议两者都具备原子性和一致性，其区别在于单次资产操作的方向性不同，跨链资产交换的单次操作具备双向性，即资产能从每一方转移到另一方，而跨链资产转移的单次操作具备单向性，即资产只能从一方转移到另一方。

2.2.1 跨链资产交换协议

跨链资产交换分为中心化的和去中心化的跨链资产交换。中心化的跨链资产交换有Coinbase、Binance等，交易费用较高，交易活动缺乏公开的可核查性，容易导致虚假交易量和受到黑客的攻击[39]。去中心化的跨链资产交换支持不同类型的数字资产的交换。目前去中心化的跨链资产交换是跨链资产交换协议的主流研究方向。基于哈希锁定技术、侧链机制、中继机制等主流跨链技术，出现了XCLAIM[40]、NCASP（novel hash-time-lock-contract based cross-chain token swap mechanism）[41]、AC^{3}WN（atomic cross chain commitment witness network）[42]、3PP（three-phase protocol）[43]、Relay Swap[44]等实现去中心化跨链资产交换的跨链资产交换协议。

XCLAIM协议[40]由Zamyatin等人提出，通过发行

表3 跨链通信协议对比分析

Table 3 Comparison and analysis between cross-chain communication protocols

协议	跨链技术	可验证性	安全性	隐私性	可扩展性	跨链类型	局限性
IBC[31]	中继	支持	中	不支持	中	同构	跨链通信开销大
MBCCP[32]	中继	不支持	高	支持	低	同构	无数据验证机制
XCMP[33]	中继	支持	高	不支持	中	同构	无具体实现
IBTP[34]	中继	支持	中	支持	高	同构+异构	无交易有效性验证机制
周期性委员会轮换协议[35]	中继与公证人	支持	中	不支持	低	同构+异构	未考虑恶意请求造成的广播风暴风险
三阶段跨链通信协议[36]	中继	不支持	低	不支持	中	同构	安全性较差
跨链通信服务协议[37]	中继	支持	中	不支持	中	同构	无激励机制、性能较差

资产代币的方式在现有区块链上实现跨链资产交易。XCLAIM协议由支持区块链、发行区块链、保险库和智能合约组成。其中，支持区块链是现有区块链，比如比特币等。发行区块链是基于支持区块链发行资产代币的区块链，比如以太坊等。保险库是一个不可信的第三方中介，负责完成资产的锁定与赎回。智能合约负责对资产进行锁定和释放操作的验证。XCLAIM协议流程如图3所示。XCLAIM协议由发布阶段、转移/交换阶段和赎回三个阶段组成。在发布阶段中，用户将发行区块链上的资产与保险库锁定，然后基于智能合约验证锁定并在发行区块链上发布资产代币。在转移/交换阶段中，发送方和接收方在发行区块链上基于智能合约实现资产锁定，进而实现具备原子性的资产代币的转移与交换。在赎回阶段中，用户用支持区块链上的资产代币赎回发行区块链上对应的资产。

NCASP协议[41]由刘峰等人提出，基于中间账户进行资产托管和转移的方式改进哈希时间锁，使得在原有跨链交易速率不变的同时，保证了交易的安全性。引入账户体系并融合智能合约技术，实现了在以太坊和Fabric联盟链网络之间的安全无缝资产交换，无需第三方区块链介入即可实现高效安全的跨链资产交换，保证跨链资产交换的原子性、公平性和透明性。

AC^{3}WN[42]由Zakhary等人提出，基于去中心化的公证人网络，通过侧链上的智能合约对跨链资产交换的交易状态进行控制，实现去中心化原子跨链交换，确保实现原子交换的原子性和最终承诺性。公证人网络本质上相当于已有区块链的侧链。AC^{3}WN本质上依然采用了原子交换技术，因此也存在和原子交换技术一样的通信通道攻击问题，另外由于公证人网络侧链，提高了协议的复杂性，降低了性能。

3PP协议[43]由Shadab等人提出，支持通用多方跨链资产交易。3PP协议用端到端属性确保协议的一致性，实现发送方转移资金的同时接收方接收资金。3PP协议支持多方跨链资产交易的转换，将原始的多方跨链交易转换为双方跨链交易，利用哈希锁定机制在双方之间发起资产交换。

Relay Swap协议[44]由Lys等人提出，基于区块链适配器提出中继交换思路，实现去中心化原子跨链，移除AC^{3}WN方法中使用的公证人网络侧链，进一步改进基于哈希锁定机制的原子交换技术。

此外，Tian等人[45]实现一种去中心化的资产交易协议，实现不同类型资产之间的交换，并基于智能合约实现多对用户并行处理跨链资产互换的方式，提高了跨链资产交换的性能。张诗童等人[46]提出一种多方跨链协议，基于哈希锁定实现多方多链资产转移结算，但缺乏对资产互换过程中安全性的关注。Cao等人[47]基于零知识证明和哈希锁定技术提出一种资产互换匿名方案，实现交易双方之间匿名交换智能合约地址，实现对跨链资产交易过程中双方交易隐私的保护。

对以上跨链资产交换协议从跨链技术、安全性、原子性、隐私性、可扩展性、跨链类型及局限性进行对比分析，见表4。

2.2.2　跨链资产转移协议

跨链资产转移协议主要有DeXTT（deterministic cross-blockchain token transfers）协议[22]、ILP（Interledger protocol）协议[48]、Zendoo协议[49]、SuSy协议[50]、AUGP（atomic unidirectional gateway protocol）协议[51]等。

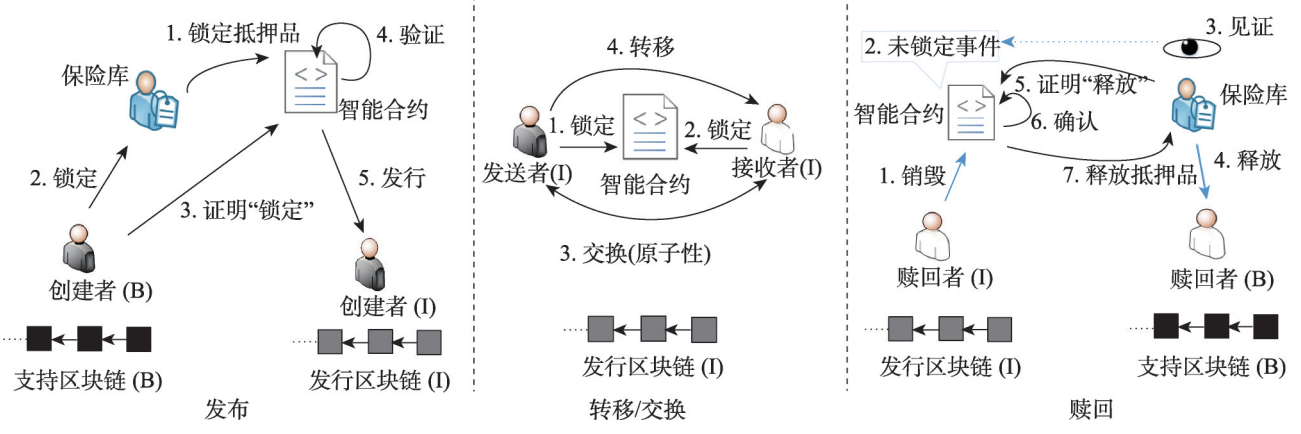


图3　XCLAIM协议

Fig.3　XCLAIM protocol

表4 跨链资产互换协议对比分析

Table 4 Comparison and analysis between cross-chain asset swap protocols

协议	跨链技术	安全性	原子性	隐私性	可扩展性	跨链类型	局限性
XCLAIM[40]	中继	高	支持	不支持	高	同构+异构	成本高,资产过度抵押
NCASP[41]	哈希锁定	高	支持	不支持	高	同构+异构	存在密钥泄露风险
AC^{3}WN[42]	哈希锁定、侧链	低	支持	不支持	中	同构	性能低
3PP[43]	哈希锁定	中	支持	不支持	低	同构	无交易容错机制
Relay Swap[44]	哈希锁定、中继	低	支持	不支持	中	同构	安全性差
去中心化资产交易协议[45]	中继	中	不支持	不支持	中	同构+异构	性能较差
多方跨链协议[46]	哈希锁定	低	支持	不支持	高	同构	无具体实现
资产互换匿名方案[47]	哈希锁定	中	支持	支持	低	同构	无具体实现

DeXTT协议[22]由Borkowski等人提出,通过claim-first transactions和deterministic witnesses确保了资产余额的最终确定性。首先,发送者将资产转移信息提供给接受者,资产转移信息包括发送方、接收方、发送数量和有效期等。然后,接受者给一个区块链发起Claim交易,记录资产转移信息。当公证人候选者们观察到Claim交易发起后,向所有区块链发起无序的Contest交易。Contest交易向所有区块链广播经过公证人候选者签名后的资产转移信息,于是每条区块链中将保存所有公证人竞争者的名单和资产转移信息。当有效期结束后,接受者发起Finalize交易,最后完成转账交易,并确定性地将奖励分配给在Contest交易中获胜的公证人。

ILP协议[48],又名Interledger协议,由Ripple公司提出,类似HTTP协议。Interledger协议中资产转移是从发送方到接收方的一系列托管传输,利用连接者(connector)连接跨链交易的发送者和接收者,在最终接受者收到资金前,协议对各方的资金进行托管锁定。该协议包括原子模式和通用模式这两种模式。在原子模式下,转账由参与者选择的一个特别公证人小组进行协调。在通用模式下,没有外部协调,而是通过有限的执行窗口、参与者激励和“反向”执行顺序使得各方之间能够安全支付,而无需共享对任何系统或机构的信任。

Zendoo协议[49]由Garoffolo等人提出,基于侧链和zk-SNARK零知识协议来构造去中心化和可验证的跨链资产转移协议,实现资产在主链和侧链之间的双向转移操作。Zendoo的跨链转移协议将主链与从主链派生的所有侧链连接起来,允许将货币发送到侧链并以安全可靠的方式接收它们,且是一个双向协议,定义了正向转移(forward transfer,FT)和反向转移(backward transfer,BT)两个基本操作。zk-SNARK允许在不泄露某些信息的情况下证明拥有这些信息,Zendoo中基于zk-SNARK为主链实现有效转移验证。

SuSy协议[50]由Pupyshev等人提出,基于Gravity协议和智能合约实现异构跨链资产转移。其中,Gravity协议是一种去中心化预言机协议,用于搭建去中心化的预言机系统。SuSy协议在源链和目标链上部署智能合约,与资产转移的发送者和接收者交互,并基于Gravity协议的预言机网络在源链和目标链中建立中继,实现对资产转移的验证。SuSy协议的跨链资产转移高度依赖预言机网络的安全性,若预言机网络遭受严重攻击,则SuSy协议的安全性将无法保障。

此外,Hardjono提出AUGP协议[51],基于区块链网关建立安全的通信通道实现具备原子性和一致性的单向跨链资产转移。其中,区块链网关指区块链中的一个节点,拥有对区块链账本的数据读写权限,可能参与区块链的共识机制,在跨链过程中定义跨链通信格式,实现跨链资产转移后的账本一致性。该协议基于网关标识公钥私钥对的身份密钥机制,在跨链资产转移过程中实现对网关身份的验证。另外,该协议基于网关对区块链账本的数据读写权限实现对跨链资产转移过程中的资产验证和状态验证。Sigwart等人提出Sigwart协议[52],定义用于实现去中心化、安全的异构跨链资产转移协议的协议规范。该协议基于智能合约技术实现资产转移声明,并通过激励机制实现资产转移的最终确认。Pillai等人提出Burn-to-Claim协议[53],实现去中心化的跨链资产转移。该协议基于哈希锁和时间锁对资产转移条件进行验证,从而确保资产的安全性,提出跨链资产转移交易应由exit交易和entry交易组成。其中,exit交易在源链中锁定资产,并在源链中充当资产转移证明,entry交易负责在目标链上验证转移证明的有效性,以便在目标链中重新创建资产。

对以上跨链资产转移协议从跨链技术、安全性、原子性、隐私性、可扩展性、跨链类型及局限性这些方面进行对比分析，具体结果见表5。

2.3　跨链智能合约调用协议

跨链智能合约（cross-chain contracts）主要目的是对原链交易进行确认和交易，与跨链资产转移非常类似。此外，跨链智能合约还支持跨区块链调用智能合约。借助跨链智能合约，能实现区块链资产留置。资产留置是一种区块链锁定资产的能力，锁定链 X 上的资产 A，并使锁定条件取决于链 Y 上的活动。在跨链智能合约调用过程中，解决异构区块链智能合约接口不一致问题，统一智能合约的运行时环境和编程语言是实现跨链智能合约调用的两大难点。目前，为实现跨链智能合约调用，学术界相继提出Move协议[54]、UIP（universal inter-blockchain protocol）[55]、SCIP（smart contract invocation protocol）[56]、GPACT（general purpose atomic crosschain transactions）[57]等跨链智能合约调用协议。

Markus等人[30]首先引入跨链智能合约的概念，提出跨链智能合约调用框架，实现了数据的跨链传输并允许智能合约跨链调用。跨链智能合约调用框架原理如图4所示。跨链智能合约调用框架由调用者、被调用者、中间人、验证者、分发合约、调用合约六部分组成。其中，调用者是指在源链上的调用实体，被调用者是指在目标链上被调用的账户，中间人是指在源链和目标链之间传递信息的第三方。跨链智能合约调用框架中实现了分发合约和调用合约。分发合约负责注册跨链智能合约调用，保存跨链相关参数，存放代币以支付交易数据和奖励。调用合约负责转发交易，进而调用执行智能合约，并将执行结果返回。验证者用来验证中间人传递的信息。

Move协议[54]由Fynn等人提出，能够将对象和智能合约从源区块链移动到目标区块链上。Move协议实现Hyperledger Burrow和以太坊之间的链间通信，实现了不同区块链之间数据和资产的转移。Move协议将智能合约的移动操作分为Move1和Move2两个事务。在Move1事务中，智能合约的状态 c（数据或资产）在源链中被锁定，然后不会再被修改，但是事务依然可以读取被锁定的智能合约中的内容。另外用 L_c 存储智能合约要转移去的目标链。在Move2事

表5　跨链资产转移协议对比分析

Table 5　Comparison and analysis between cross-chain asset transfer protocols

协议	跨链技术	安全性	原子性	隐私性	可扩展性	跨链类型	局限性
DeXTT[22]	公证人	低	支持	不支持	中	同构	使用范围有限
Interledger[48]	公证人	低	支持	不支持	中	同构+异构	无容错机制
Zendoo[49]	侧链	高	支持	支持	低	同构	计算量大，实现难度大
SuSy[50]	中继	低	支持	不支持	中	同构+异构	无激励机制，未考虑双重支付
AUGP[51]	中继	中	支持	不支持	中	同构	无具体实现
Sigwart协议[52]	哈希锁定	中	支持	不支持	低	同构+异构	手续费较高
Burn-to-Claim[53]	哈希锁定	中	支持	不支持	低	同构	无具体实现，无事务回滚机制

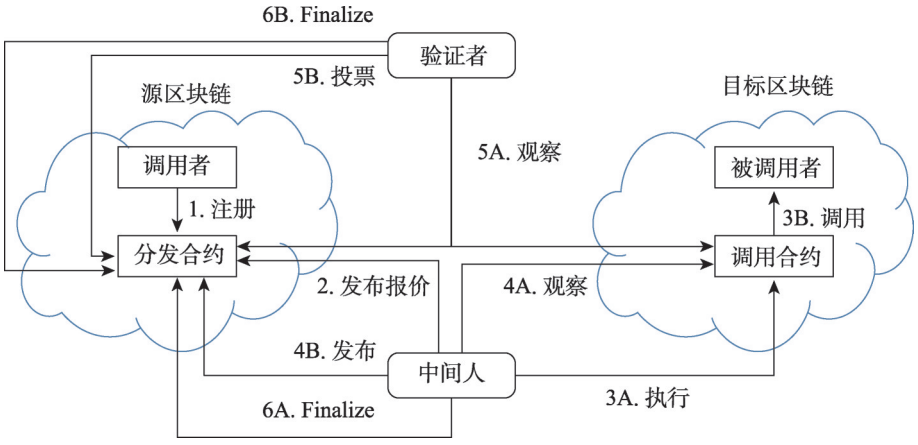


图4　跨链智能合约调用框架

Fig.4　Framework for cross-chain smart contract invocations

务中，客户端2实现验证目标链的正确性、验证区块链的默克尔根和验证c是否被锁定三大证明功能。在客户端2通过上述三大证明之后，由Move2事务在目标链上重新创建智能合约的状态c。

UIP协议[55]由Liu等人提出，应用于HyperService平台。UIP协议是一种区块链通用的互操作性协议，定义了跨链操作中各方实体要执行的动作，采用网络状态区块链（network status blockchain，NSB）和保险智能合约（insurance smart contract，ISC）两大创新设计。NSB是HyperService设计的区块链，其提供对DApp执行状态的客观和统一的视图。NSB实现行动证明（proofs of actions，PoAs），支持DApp客户端和VESes通过构建证明的方式来证明它们参与的跨链行为。ISC是运行在NSB上的智能合约，负责保证跨链操作正确执行，以NSB构建的事务状态证明作为输入，从而判断DApp执行的正确性与非法性，同时使用上述的行动证明来确定异常情况下的责任方。

SCIP协议[56]由Falazi等人提出，基于网关的方式为异构区块链提供一个同构接口，统一不同区块链智能合约的交互。SCIP网关结构分为SCIP端口、区块链访问核心层、适配器模块三部分。SCIP端口实现了一个JSON-RPC服务器提供调用、订阅、取消订阅、查询这四种方法，允许智能合约客户端调用和监视异构区块链系统的智能合约，从而实现智能合约交互。区块链访问核心层提供了处理请求和发送回调的逻辑。适配器模块是可插拔的适配器模块，由一个特定区块链的协议客户端执行特定于某个区块链的操作，比如如何处理调用智能合约，如何编码/解码参数，如何监控和查询事件等。

GPACT协议[57]由Robinson等人提出，基于BLS阈值签名（BLS threshold signatures）、协调合约（coordination contracts）、动态代码分析和签名嵌套事务、合约锁定的原子跨链交易技术[58-59]实现跨链智能合约调用，在区块链间的应用层和合约层提供具备原子性和一致性的跨链合约调用功能。其中，原子跨链交易技术是区块链layer1技术，需要更改以太网客户端软件，不适用于以太网客户端软件无法修改的应用。上述研究只针对以太坊平台，如何将上述研究提出的原子跨链技术和GPACT协议用于非以太网区块链系统，进而实现异构区块链跨链是一项重大挑战。

目前在跨链智能合约方面的研究主要关注跨链智能合约调用的实现，对以上跨链智能合约调用协议从安全性、隐私性、可扩展性、原子性、跨链类型和局限性这些方面进行对比分析，见表6。

3 跨链协议关键设计原则

综前所述，跨链协议主要包含跨链通信协议、跨链资产交易协议和跨链智能合约调用协议。三者共同构成区块链跨链互操作领域的协议规范。通过对跨链协议的设计原则，即可扩展性、安全性和隐私性进行详细阐述，进一步明确跨链协议的技术要求与设计规范。

3.1 安全性

在跨链互操作过程中，跨链协议的安全性是一个值得关注的问题。跨链协议中需要对涉及到的数据对象、资产对象进行保护，确保在跨链过程中安全、可靠、可信地实现数据或资产的链间转移或链间互换。为设计安全性高的跨链协议，需要满足以下设计原则：

（1）资产保护机制。资产保护机制重点关注跨链资产转移和跨链资产互换过程中对资产的保护，比如对双花攻击（double-spend attack）、竞争条件攻击（race condition attack）、跨链重放攻击（cross-chain replay attacks）等安全问题[60]的处理。在跨链资产转移中的资产安全问题关键在于如何防止伪造资产转移并且资产转移只能发生一次。另外在跨链资产互换中的资产安全问题关键在于某条链发生重构的情况下，是否能够依然保持两条链的资产总量不变。Pang[61]通过改进PoS（proof of stack）共识提出MPoS（multi-token proof of stake）共识，用于中继跨链中的

表6 跨链智能合约调用协议对比分析

Table 6 Comparison and analysis between cross-chain smart contract call protocols

协议	安全性	隐私性	可扩展性	原子性	跨链类型	局限性
跨链智能合约调用框架[30]	中	不支持	中	不支持	同构	跨链调用开销大，无激励机制
Move[54]	中	不支持	中	支持	同构+异构	性能较差，手续费高
UIP[55]	高	不支持	高	支持	同构	实现难度较大
SCIP[56]	低	不支持	中	不支持	同构+异构	安全性低
GPACT[57]	高	不支持	低	支持	同构	使用范围有限

资产安全性。Hardjono等人[62]为实现安全的资产交换，基于现有的公钥证书体系提出一种面向虚拟资产和虚拟资产服务提供商的公钥管理方案，实现密钥的安全交换和个人隐私信息的保护。

（2）超时处理机制。跨链协议在执行跨链交易时，在遇到超时的交易时应当进行适当的处理，从而避免交易失败影响跨链协议的后续过程。因此，跨链协议应设置超时处理机制，当所进行的跨链交易中的操作未在限定时间内响应时，应视为操作失败，回滚已经执行的操作，将交易状态恢复到之前的状态中。

（3）可信性。在跨链场景中，各自独立的区块链网络需要相互获取对方链上的数据，由于它们并没有参与对方区块链的共识流程，如何保证获得的数据可信是一个技术难度。因此需要引入额外的可信证明对跨链交易的合法性和有效性进行验证，从而实现跨链协议的可信性。目前公证人机制[63]、SPV验证[64]是常用的跨链交易验证方式。

（4）可审计性。跨链协议中的跨链交易中有着不同的跨链行为，其在跨链过程中会对数据信息、资产信息进行修改。而恶意的跨链行为会造成数据、资产的损失，因此跨链协议需要提供对跨链行为的记录，从而实现跨链行为的可审计、可追溯。Belchior等人[65]设计了具备原子性、一致性、可持久性和隔离性的区块链互操作性中间件，用于两方跨链资产交易，提供可审计日志功能。雷志伟等人[66]提出基于双链并行模式实现监管链，从而实现跨链的可审计性。

（5）崩溃恢复机制。在区块链跨链互操作过程中，网络的可用性会影响跨链成功与否，因此当遇到网络崩溃时跨链协议应有崩溃恢复机制对崩溃的状态进行修复。

（6）数据一致性。在区块链跨链互操作过程中，数据一致性指在跨链协议执行跨链交易时如何保证不同区块链上的数据能够达成一致。跨链协议为保证跨链交易中各自链上交易执行后的数据一致性，需要对事务进行管理，比如跨链资产交易协议中让所有参与交易的区块链对资产的操作同时成功或者同时失败。在跨链协议的设计过程中，借鉴传统分布式事务提出的两阶段提交协议（two phase commit，2PC）和三阶段提交协议（three phase commit，3PC），这两种分布式一致性算法对跨链协议的数据一致性机制进行设计，实现分布式事务，以确保不同链上的数据正确被修改并被记录入区块中，跨链交易完成后不同区块链之间达成数据一致。

3.2　可扩展性

区块链的可扩展性问题指的是由于区块大小限制、共识时间长、每秒交易数（TPS）限制等问题造成的区块链交易性能低下以及区块链存储空间急剧加大[67]。目前，区块链可扩展性的瓶颈包括性能扩展和功能扩展两方面，在性能扩展上主要关注于如何提升区块链的性能效率，在功能扩展上主要关注扩展区块链的功能进而增强区块链服务能力[68]。区块链系统的可扩展性的不足在一定程度上影响了建立在区块链之上的服务的可扩展性，因此区块链跨链协议在设计上需要考虑可扩展性的需求。为了设计具备可扩展性的区块链跨链协议，需要满足以下设计原则：

（1）应用场景多元化。实际应用业务中存在跨部门、跨业务、跨架构、跨行业的跨链需求，为此跨链协议的设计需要考虑到应用场景多元化的问题，通过对跨链交互模型的抽象设计，提炼出关键的跨链参数，以应对复杂多变的跨链场景，从而提高系统的可扩展性。如郑建辉等人[69]将跨链场景抽象为资产交换、资产转移、信息付费和信息交互四类，针对这四种跨链交互场景分别设计智能合约模板，从而提高可扩展性。

（2）松耦合架构。在跨链协议的设计中，应降低跨链协议与区块链平台的耦合度，扩大跨链协议的应用范围，从而提高可扩展性。类似互联网通信协议中的端到端原则，在跨链交易的转移过程中跨链协议无需关心内部的架构设计，对被移动的资产或数据的价值不可知，从而允许跨链协议的设计更加高效、快速和可靠。当跨链协议中的跨链通道或者锚定节点受损时，区块链不会受到影响，依然可以正常运行。

（3）并行架构。基于侧链或中继的跨链协议在设计跨链架构时均采取了并行架构设计，通过并行的方式扩展了区块链的交易性能与存储空间，如Cosmos中的中心链（hub）与平行链（zone），Polkadot中的中继链（relay-chain）和平行链（parachains）。戴波等人[70]将区块链节点进行多角色划分，通过主链和子链的并行架构进一步提高可扩展性。

（4）链下通道。跨链协议的链下通道设计包括微支付通道和链下存储通道两种方式，如比特币系统中的闪电网络[71]、以太坊系统中的雷电网络技术[72]

和基于IPFS(interplanetary file system)和Swarm的链下存储[73],两者均可通过链下通道的方式可以将支付或存储转移到链下,在支付和存储上增强跨链协议的性能,进一步提高跨链协议的可扩展性。

3.3 隐私性

欧盟通用数据保护条例(general data protection regulation, GDPR)要求涉及安全和隐私数据的系统支持不同级别的机密性、安全性和隐私性保证。而区块链中的隐私分为身份隐私和交易隐私两类。身份隐私代表用户身份信息与区块链地址之间的隐私关联关系。交易隐私指在区块链中存储的交易记录及其背后隐藏的信息,比如比特币区块链中记录了用户之间的转账记录[74]。目前,较少跨链协议考虑到对身份隐私和交易隐私的保护。比如当前大部分跨链交易的候选方案未提供交易隐私保护机制,交易双方的身份以及交易信息均是公开的[75]。而在区块链跨链互操作过程中,对用户的身份隐私与交易隐私进行保护是不可或缺的,为设计具备隐私性的跨链协议,需要满足以下设计原则:

(1)交易信息隐藏机制。跨链协议在进行跨链交易时需要对关键的交易信息进行隐藏处理,通过零知识证明、混币机制、代理重加密、同态加密、环签名等密码学技术加密区块链账本中记录的交易信息,保证账本正确性的可验证,从而防止攻击方获得完整的交易信息,增强跨链交易的匿名性。Stone[76]基于零知识证明和Merkle树实现交易验证,从而保护交易隐私。

(2)网络数据混淆处理。为了预防攻击者利用网络拓扑来获取用户的身份隐私信息,跨链协议需对网络数据进行混淆处理,比如使用基于洋葱路由和大蒜路由的混淆网络对系统进行加固,从而保护区块链系统中的用户IP地址的隐私安全。

(3)数据访问控制。在跨链过程中为保护区块链上的数据安全,任何供区块链外部实体访问的数据信息都必须在经过授权后通过特定的接口才能被访问。基于主流身份认证协议、加密校验、零知识证明、属性基加密等方式实现数据访问控制策略,从而确保区块链的数据隐私。Fabric的通道机制实现不同场景下的数据访问控制,并且实现业务数据隔离,通过限制消息的传播范围保护了用户隐私。如Wang等人[77]基于跨链技术解决医疗信息孤岛问题,并通过对访问权限的控制保护病人的就医隐私信息。

对以上三点跨链协议关键设计原则进行分析,相关内容总结如表7。

4 研究展望

对跨链协议的研究是构建区块链跨链应用生态的必经之路,其中的研究重点是跨链协议的安全性、可扩展性和隐私性。针对当前跨链协议研究的不足,未来的研究方向主要包括以下五方面:

(1)跨链协议的统一标准。区块链互操作标准,又称区块链跨链标准,是基于跨链实现区块链互操作性的标准规范,旨在创建所有区块链通用的标准化事务格式和语法[78]。IEEE、ITU、ISU、中国区块链技术和产业发展论坛等国内外相关专业机构提出了若干跨链标准。但目前的跨链协议没有遵守统一的跨链标准,无法形成统一的跨链体系。因此为了构建可用性强、扩展性强、安全性高、隐私性好、高性能、高效率的区块链链联网生态系统,促进数字经济新型基础设施建设,在未来的跨链协议研究中应重视对跨链协议统一标准的研究。

(2)跨链协议的安全性。跨链通信互操作协议如何验证通信传输数据的正确性,如何确保跨链通信过程中的数据安全性,采取何种同步手段来保持数据一致性是未来研究关注的重点方向。跨链资产交易互操作协议如何实现资产安全性并确保交易的原子性也是未来研究关注的重点方向。

(3)跨链协议的性能与应用。目前跨链协议的

表7 跨链协议关键设计原则总结

Table 7 Summary of key design principles of cross-chain protocols

相关文献	类型	具体内容	解决方案
[31-33,36-37,40-41,61-66]	安全性	资产保护机制、超时处理机制、数据可信验证、可审计性、崩溃恢复机制、数据一致性	公证人机制、SPV验证、2PC协议、3PC协议
[46,49,54,56,70-73]	可扩展性	应用场景多元化、松耦合架构、并行架构、链下通道	侧链、中继、微支付通道、链下存储通道
[34,47,49,75-77]	隐私性	交易信息隐藏机制、网络数据混淆处理、数据访问控制	零知识证明、混币机制、代理重加密、同态加密、环签名、混淆网络、属性基加密

性能存在一定瓶颈,在实际应用场景中的应用能力有待加强。因此,提升跨链协议的性能与应用能力将是今后研究的一个重要方向。

(4)跨链协议的隐私性。跨链协议的隐私性涉及交易隐私和用户隐私,而当前跨链协议侧重于对安全性、可扩展性的分析研究,缺少对隐私性的关注,未来对跨链协议的研究应该考虑到隐私性方面的设计。

(5)跨链行为审计与故障处理机制。在跨链协议的实现过程中,应实现对跨链行为的审计,对各方的恶意行为进行检测与处理,最终加强并优化激励机制以激励各方遵守协议。另外跨链互操作协议如何处理跨链过程的网络故障,如何恢复发生故障后的交易信息也是有待解决的难题。

(6)跨链智能合约应用。智能合约有增强区块链互操作性的潜力,但目前尚未重视智能合约在区块链互操作性领域的作用,跨链智能合约调用协议的研究近几年刚刚兴起。在未来设计跨链协议的过程中,需要针对跨链智能合约调用协议,研究如何通过跨链智能合约调用实现跨链事务处理和跨链查询处理,结合不同区块链的功能,实现跨组织、跨业务的功能互通,进而构建区块链跨链应用。

5　结束语

随着区块链技术的发展,区块链跨链互操作需求不断增长,实现区块链的链间互操作性必将是区块链未来发展的必经之路。区块链跨链互操作的最终目的在于构建链联网,即构建跨链应用,从而实现各个区块链的互联互通。实现不同区块链之间的数据互通、价值互通和功能互通将破除异构区块链之间的联通壁垒,从根本上解决区块链的可扩展性问题,扩展区块链的应用范围。因此,为实现区块链跨链互操作,构建跨链协议将是区块链的重点研究方向。本文总结和分析了区块链互操作性的定义以及跨链技术和跨链架构,并对跨链通信协议、跨链资产交易协议、跨链智能合约调用协议的研究现状进行总结分析,最后指出跨链协议的关键设计原则和未来研究方向。

参考文献:

[1] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述: 原理、进展与应用[J]. 通信学报, 2020, 41(1): 134-151.
ZENG S Q, HUO R, HUANG T, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020, 41(1): 134-151.

[2] 熊啸, 李雷孝, 高静, 等. 区块链在车联网数据共享领域的研究进展[J]. 计算机科学与探索, 2022, 16(5): 1008-1024.
XIONG X, LI L X, GAO J, et al. Research progress of blockchain in Internet of vehicles data sharing[J]. Journal of Frontiers of Computer Science and Technology, 2022, 16 (5): 1008-1024.

[3] 姚前, 张大伟. 区块链系统中身份管理技术研究综述[J]. 软件学报, 2021, 32(7): 2260-2286.
YAO Q, ZHANG D W. Overview of research on identity management technology in blockchain systems[J]. Journal of Software, 2021, 32(7): 2260-2286.

[4] 周如月, 钱良. 基于区块链信用体系的分布式数字版权管理机制[J]. 计算机应用研究, 2020, 37(6): 1794-1798.
ZHOU R Y, QIAN L. Blockchain based digital right management for distributed content delivery network[J]. Application Research of Computers, 2020, 37(6): 1794-1798.

[5] 王晨旭, 程加成, 桑新欣, 等. 区块链数据隐私保护: 研究现状与展望[J]. 计算机研究与发展, 2021, 58(10): 2099-2119.
WANG C X, CHENG J C, SANG X X, et al. Data privacy-preserving for blockchain: state of the art and trends[J]. Journal of Computer Research and Development, 2021, 58 (10): 2099-2119.

[6] 李芳, 李卓然, 赵赫. 区块链跨链技术进展研究[J]. 软件学报, 2019, 30(6): 1649-1660.
LI F, LI Z R, ZHAO H. Research on the progress in cross-chain technology of blockchains[J]. Journal of Software, 2019, 30(6): 1649-1660.

[7] 徐卓嫣, 周轩. 跨链技术发展综述[J]. 计算机应用研究, 2021, 38(2): 341-346.
XU Z Y, ZHOU X. Survey on crosschain technology[J]. Application Research of Computers, 2021, 38(2): 341-346.

[8] 路爱同, 赵阔, 杨晶莹, 等. 区块链跨链技术研究[J]. 信息网络安全, 2019, 19(8): 83-90.
LU A T, ZHAO K, YANG J Y, et al. Research on cross-chain technology of blockchain[J]. Netinfo Security, 2019, 19(8): 83-90.

[9] VO H T, WANG Z Y, KARUNAMOORTHY D, et al. Internet of blockchains: techniques and challenges ahead [C]//Proceedings of the 2018 IEEE International Conference on Internet of Things and Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data, 2018: 1574-1581.

[10] 戴炳荣, 姜胜明, 李顿伟, 等. 基于改进PageRank算法的跨链公证人机制评价模型[J]. 计算机工程, 2021, 47(2): 26-31.
DAI B R, JIANG S M, LI D W, et al. Evaluation model of cross-chain notary mechanism based on improved PageRank algorithm[J]. Computer Engineering, 2021, 47(2): 26-31.

[11] 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]//Proceedings of the 2nd International Conference on Blockchain and Trustworthy Systems, Dali, Aug 6-7, 2020. Singapore: Springer, 2020: 218-230.

[12] GAŽI P, KIAYIAS A, ZINDROS D. Proof-of-stake sidechains[C]//Proceedings of the 2019 IEEE Symposium on Security and Privacy, San Francisco, May 19-23, 2019. Piscataway: IEEE, 2019: 139-156.

[13] FRAUENTHALER P, SIGWART M, SPANRING C, et al. Testimonium: a cost-efficient blockchain relay[J]. arXiv:2002.12837, 2020.

[14] SHI L, GUO Z. Baguena: a practical proof of stake protocol with a robust delegation mechanism[J]. Chinese Journal of Electronics, 2020, 29(5): 887-898.

[15] GUDGEON L, MORENO-SANCHEZ P, ROOS S, et al. SoK: layer-two blockchain protocols[C]//LNCS 12059: Proceedings of the 24th International Conference on Financial Cryptography and Data Security, Kota Kinabalu, Feb 10-14, 2020. Cham: Springer, 2020: 201-226.

[16] WEGNER P. Interoperability[J]. ACM Computing Surveys, 1996, 28(1): 285-287.

[17] VERNADAT F B. Interoperable enterprise systems: architectures and methods[J]. IFAC Proceedings Volumes, 2006, 39(3): 13-20.

[18] KOENS T, POLL E. Assessing interoperability solutions for distributed ledgers[J]. Pervasive and Mobile Computing, 2019, 59: 101079.

[19] BUTERIN V. Chain interoperability[EB/OL]. (2016)[2022-02-18]. https://allquantor.at/blockchainbib/pdf/buterin2016chain.pdf.

[20] JIN H, DAI X H, XIAO J. Towards a novel architecture for enabling interoperability amongst multiple blockchains[C]//Proceedings of the 2018 38th IEEE International Conference on Distributed Computing Systems, Vienna, Jul 2-6, 2018. Washington: IEEE Computer Society, 2018: 1203-1211.

[21] ABEBE E, BEHL D, GOVINDARAJAN C, et al. Enabling enterprise blockchain interoperability with trusted data transfer(industry track)[C]//Proceedings of the 20th International Middleware Conference Industrial Track, Davis, Dec 9-13, 2019. New York: ACM, 2019: 29-35.

[22] BORKOWSKI M, SIGWART M, FRAUENTHALER P, et al. DeXTT: deterministic cross-blockchain token transfers[J]. IEEE Access, 2019, 7: 111030-111042.

[23] SCHULTE S, SIGWART M, FRAUENTHALER P, et al. Towards blockchain interoperability[C]//Proceedings of the 2019 International Conference on Business Process Management, Vienna, Sep 1-6, 2019. Cham: Springer, 2019: 3-10.

[24] BELCHIOR R, VASCONCELOS A, GUERREIRO S, et al. A survey on blockchain interoperability: past, present, and future trends[J]. arXiv:2005.14282, 2020.

[25] 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, Maui, Jan 7-10, 2020: 1-10.

[26] LAFOURCADE P, LOMBARD-PLATET M. About blockchain interoperability[J]. Information Processing Letters, 2020, 161: 105976.

[27] 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(6): 294-302.
YE S J, WANG X Y, XU C C, et al. BitXHub: side-relay chain based heterogeneous blockchain interoperable platform[J]. Computer Science, 2020, 47(6): 294-302.

[28] ZAMYATIN A, AL-BASSAM M, ZINDROS D, et al. SoK: communication across distributed ledgers[C]//LNCS 12675: Proceedings of the 25th International Conference on Financial Cryptography and Data Security, Mar 1-5, 2021. Cham: Springer, 2021: 3-36.

[29] HERLIHY M. Atomic cross-chain swaps[C]//Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, Egham, Jul 23-27, 2018. New York: ACM, 2018: 245-254.

[30] NISSL M, SALLINGER E, SCHULTE S, et al. Towards cross-blockchain smart contracts[C]//Proceedings of the 2021 IEEE International Conference on Decentralized Applications and Infrastructures, Aug 23-26, 2021. Piscataway: IEEE, 2021: 85-94.

[31] GOES C. The interblockchain communication protocol: an overview[J]. arXiv:2006.15918, 2020.

[32] SHE W, GU Z, LIU W, et al. A channel matching scheme for cross-chain[J]. International Journal of Embedded Systems, 2020, 12(4): 500-509.

[33] BURDGES J, CEVALLOS A, CZABAN P, et al. Overview of Polkadot and its design considerations[J]. arXiv:2005.13456, 2020.

[34] WANG H, HE D, GAO Y, et al. Research on data verification and exchange of heterogeneous blockchains for electricity application[C]//Proceedings of the 2nd International Conference on Artificial Intelligence and Computer Science, Hangzhou, Jul 25-26, 2020: 012154.

[35] WU Z H, XIAO Y, ZHOU E Y, et al. A solution to data accessibility across heterogeneous blockchains[C]//Proceedings of the 26th IEEE International Conference on Parallel and Distributed Systems, Hong Kong, China, Dec 2-4, 2020. Piscataway: IEEE, 2020: 414-421.

[36] LUO K, YU W, HAFIZ M A, et al. A multiple blockchains architecture on inter-blockchain communication[C]//Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion, Lisbon, Jul 16-20, 2018. Piscataway: IEEE, 2018: 139-145.

[37] 康博涵, 章宁, 朱建明. 基于区块链的智能服务交易跨链服务框架与通信机制[J]. 网络与信息安全学报, 2021, 7(3): 105-114.
KANG B H, ZHANG N, ZHU J M. Research on inter-

blockchain service framework and communication mechanism based on smart service transaction[J]. Chinese Journal of Network and Information Security, 2021, 7(3): 105-114.

[38] HERLIHY M, LISKOV B, SHRIRA L. Cross-chain deals and adversarial commerce[J]. arXiv:1905.09743, 2019.

[39] WERNER S M, PEREZ D, GUDGEON L, et al. SoK: decentralized finance (DeFi)[J]. arXiv:2101.08778, 2021.

[40] ZAMYATIN A, HARZ D, LIND J, et al. XCLAIM: trustless, interoperable, cryptocurrency-backed assets[C]//Proceedings of the 2019 IEEE Symposium on Security and Privacy, San Francisco, May 19-23, 2019. Piscataway: IEEE, 2019: 193-210.

[41] 刘峰, 张嘉淏, 周俊杰, 等. 基于改进哈希时间锁的区块链跨链资产交互协议[J]. 计算机科学, 2022, 49(1): 336-344.
LIU F, ZHANG J H, ZHOU J J, et al. Novel hash-time-lock-contract based cross-chain token swap mechanism of blockchain[J]. Computer Science, 2022, 49(1): 336-344.

[42] ZAKHARY V, AGRAWAL D, ABBADI A E. Atomic commitment across blockchains[J]. arXiv:1905.02847, 2019.

[43] SHADAB N, HOUSHMAND F, LESANI M. Cross-chain transactions[C]//Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency, Toronto, May 2-6, 2020. Piscataway: IEEE, 2020: 1-9.

[44] LYS L, MICOULET A, POTOP-BUTUCARU M. Atomic cross chain swaps via relays and adapters[C]//Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems, London, Sep 25, 2020. New York: ACM, 2020: 59-64.

[45] TIAN H, XUE K, LUO X, et al. Enabling cross-chain transactions: a decentralized cryptocurrency exchange protocol [J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 3928-3941.

[46] 张诗童, 秦波, 郑海彬. 基于哈希锁定的多方跨链协议研究[J]. 网络空间安全, 2018, 9(11): 57-62.
ZHANG S T, QIN B, ZHENG H B. Research on the protocol of multiple cross-chains based on the hash lock[J]. Information Security and Technology, 2018, 9(11): 57-62.

[47] CAO L, WAN Z. Anonymous scheme for blockchain atomic swap based on zero-knowledge proof[C]//Proceedings of the 2020 IEEE International Conference on Artificial Intelligence and Computer Applications, Dalian, Jun 27-29, 2020. Piscataway: IEEE, 2020: 371-374.

[48] HOPE-BAILIE A, THOMAS S. Interledger: creating a standard for payments[C]//Proceedings of the 25th International Conference Companion on World Wide Web, Montréal, Apr 11-15, 2016. New York: ACM, 2016: 281-282.

[49] GAROFFOLO A, KAIDALOV D, OLIYNYKOV R. Zendoo: a zk-SNARK verifiable cross-chain transfer protocol enabling decoupled and decentralized sidechains[C]//Proceedings of the 40th IEEE International Conference on Distributed Computing Systems, Singapore, Nov 29-Dec 1, 2020. Piscataway: IEEE, 2020: 1252-1262.

[50] PUPYSHEV A, DZHAFAROV E, SAPRANIDI I, et al. SuSy: a blockchain-agnostic cross-chain asset transfer gateway protocol based on gravity[J]. arXiv:2008.13515, 2020.

[51] HARDJONO T. Blockchain gateways, bridges and delegated hash-locks[J]. arXiv:2102.03933, 2021.

[52] SIGWART M, FRAUENTHALER P, SPANRING C, et al. Decentralized cross-blockchain asset transfers[J]. arXiv:2004.10488, 2020.

[53] PILLAI B, BISWAS K, HÓU Z, et al. The burn-to-claim cross-blockchain asset transfer protocol[C]//Proceedings of the 25th International Conference on Engineering of Complex Computer Systems, Singapore, Oct 28-31, 2020. Piscataway: IEEE, 2020: 119-124.

[54] FYNN E, BESSANI A, PEDONE F. Smart contracts on the move[C]//Proceedings of the 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Valencia, Jun 29-Jul 2, 2020. Piscataway: IEEE, 2020: 233-244.

[55] LIU Z T, XIANG Y X, SHI J, et al. HyperService: interoperability and programmability across heterogeneous blockchains[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, Nov 11-15, 2019. New York: ACM, 2019: 549-566.

[56] FALAZI G, BREITENBÜCHER U, DANIEL F, et al. Smart contract invocation protocol (SCIP): a protocol for the uniform integration of heterogeneous blockchain smart contracts[C]//LNCS 12127: Proceedings of the 32nd International Conference on Advanced Information Systems Engineering, Grenoble, Jun 8-12, 2020. Cham: Springer, 2020: 134-149.

[57] ROBINSON P, RAMESH R. General purpose atomic crosschain transactions[C]//Proceedings of the 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services, Paris, Sep 27-30, 2021. Piscataway: IEEE, 2021: 61-68.

[58] ROBINSON P, RAMESH R, BRAINARD J, et al. Atomic crosschain transactions white paper[J]. arXiv:2003.00903, 2020.

[59] ROBINSON P, RAMESH R, JOHNSON S. Atomic cross-chain transactions for ethereum private sidechains[J]. Blockchain: Research and Applications, 2022, 3(1): 100030.

[60] 田国华, 胡云瀚, 陈晓峰. 区块链系统攻击与防御技术研究进展[J]. 软件学报, 2021, 32(5): 1495-1525.
TIAN G H, HU Y H, CHEN X F. Research progress on attack and defense techniques in block-chain system[J]. Journal of Software, 2021, 32(5): 1495-1525.

[61] PANG Y. A new consensus protocol for blockchain interoperability architecture[J]. IEEE Access, 2020, 8: 153719-153730.

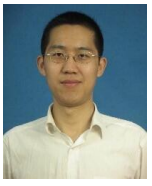
[62] HARDJONO T, LIPTON A, PENTLAND A. Toward a public-key management framework for virtual assets and virtual asset service providers[J]. The Journal of FinTech, 2021, 1(1): 2050001.

[63] ZHAO J, YANG H. Social-aware cross-chain authentication strategy in mobile edge computing[C]//Proceedings of the 9th IEEE International Conference on Information, Communication and Networks, Xi'an, Nov 25-28, 2021. Piscataway: IEEE, 2021: 170-174.
[64] RAY P P, KUMAR N, DASH D. BLWN: blockchain-based lightweight simplified payment verification in IoT-assisted e-healthcare[J]. IEEE Systems Journal, 2021, 15(1): 134-145.
[65] BELCHIOR R, VASCONCELOS A, CORREIA M, et al. Hermes: fault-tolerant middleware for blockchain interoperability[J]. Future Generation Computer Systems, 2022, 129: 236-251.
[66] 雷志伟, 朱义, 张健, 等. 一种可监管的区块链跨链平台设计[J]. 计算机与数字工程, 2021, 49(12): 2544-2550.
LEI Z W, ZHU Y, ZHANG J, et al. Design of a supervised blockchain cross chain platform[J]. Computer and Digital Engineering, 2021, 49(12): 2544-2550.
[67] ZHOU Q, HUANG H, ZHENG Z, et al. Solutions to scalability of blockchain: a survey[J]. IEEE Access, 2020, 8: 16440-16455.
[68] 潘晨, 刘志强, 刘振, 等. 区块链可扩展性研究: 问题与方法[J]. 计算机研究与发展, 2018, 55(10): 2099-2110.
PAN C, LIU Z Q, LIU Z, et al. Research on scalability of blockchain technology: problems and methods[J]. Journal of Computer Research and Development, 2018, 55(10): 2099-2110.
[69] 郑建辉, 林飞龙, 陈中育, 等. 基于联盟自治的区块链跨链机制[J]. 计算机应用(2022-01-19)[2022-02-18]. https://kns.cnki.net/kcms/detail/51.1307.TP.20220117.1746.003.html.
ZHENG J H, LIN F L, CHEN Z Y, et al. Cross chain mechanism of blockchain based on alliance autonomy[J/OL]. Journal of Computer Application(2022-01-19)[2022-02-18]. https://kns.cnki.net/kcms/detail/51.1307.TP.20220117.1746.003.html.
[70] 戴波, 赖旬阳, 胡凯, 等. 基于多角色节点的区块链可扩展方案研究与设计[J]. 浙江工业大学学报, 2021, 49(5): 487-493.
DAI B, LAI X Y, HU K, et al. Research and design of scalable blockchain scheme based on multi-role nodes[J]. Journal of Zhejiang University of Technology, 2021, 49(5): 487-493.
[71] SERES I A, GULYÁS L, NAGY D A, et al. Topological analysis of bitcoin's lightning network[C]//Proceedings of the 1st International Conference on Mathematical Research for Blockchain Economy, Santorini, May 6-9, 2019. Cham: Springer, 2020: 1-12.
[72] What is the raiden network[EB/OL]. (2019)[2022-02-18]. https://raiden.network/101.html.
[73] HUANG H, LIN J, ZHENG B, et al. When blockchain meets distributed file systems: an overview, challenges, and open issues[J]. IEEE Access, 2020, 8: 50574-50586.
[74] 康海燕, 邓婕. 区块链数据隐私保护研究综述[J]. 山东大学学报(理学版), 2021, 56(5): 92-110.
KANG H Y, DENG J. Survey on blockchain data privacy protection[J]. Journal of Shandong University (Natural Science), 2021, 56(5): 92-110.
[75] DESHPANDE A, HERLIHY M. Privacy-preserving cross-chain atomic swaps[C]//LNCS 12063: Proceedings of the 2020 International Conference on Financial Cryptography and Data Security, Malaysia, Feb 14, 2020. Cham: Springer, 2020: 540-549.
[76] STONE D. Trustless, privacy-preserving blockchain bridges [J]. arXiv:2102.04660, 2021.
[77] WANG Y, HE M X. CPDS: a cross-blockchain based privacy-preserving data sharing for electronic health records [C]//Proceedings of the 2021 IEEE 6th International Conference on Cloud Computing and Big Data Analytics, Chengdu, Apr 24-26, 2021. Piscataway: IEEE, 2021: 90-99.
[78] HARDJONO T, LIPTON A, PENTLAND A. Toward an interoperability architecture for blockchain autonomous systems[J]. IEEE Transactions on Engineering Management, 2020, 67(4): 1298-1309.

孟博(1974—),男,河北石家庄人,博士,教授,主要研究方向为区块链安全、隐私保护等。
MENG Bo, born in 1974, Ph.D., professor. His research interests include blockchain security, privacy protection, etc.

王乙丙(1997—),男,湖北黄冈人,硕士研究生,主要研究方向为区块链跨链协议、隐私保护等。
WANG Yibing, born in 1997, M.S. candidate. His research interests include blockchain cross-chain protocol, privacy protection, etc.

赵璨(1998—),女,河北承德人,硕士研究生,主要研究方向为法律合约和智能合约。
ZHAO Can, born in 1998, M.S. candidate. Her research interests include legal contract and smart contract.



王德军(1974—),男,湖北荆门人,博士,副教授,主要研究方向为知识图谱、对话系统等。
WANG Dejun, born in 1974, Ph.D., associate professor. His research interests include knowledge graph, dialogue system, etc.

麻斌豪(1998—),男,浙江温州人,硕士研究生,主要研究方向为区块链跨链技术。
MA Binhao, born in 1998, M.S. candidate. His research interest is blockchain cross-chain technology.