·计算机与信息技术·

区块链跨链技术发展及应用研究综述

何　帅,黄襄念*,陈晓亮
(西华大学计算机与软件工程学院,四川 成都 610039)

摘　要: 区块链经过十多年的深入发展,已经形成了具有不同特性、适用于不同应用场景的区块链网络。由于区块链的孤立性以及链与链之间的高度异构化,因此区块链之间的数据流通、价值转移成为了阻碍区块链技术广泛落地应用的技术瓶颈。区块链的跨链技术是实现区块链互联互通、提升区块链互操作性与可扩展性的重要技术手段。针对区块链间跨链交互难的问题,文章对区块链的跨链技术的发展和应用进行研究,阐述了跨链的基础原理,介绍了现有的跨链核心技术,分析了跨链技术面临的技术难点,总结了跨链技术的安全性风险和实际应用,探讨了当前跨链技术面临的挑战和未来的发展方向。

关键词: 区块链;跨链技术;互操作性;价值转移

中图分类号: TP393.09; TP311.13　　**文献标志码:** A　　**文章编号:** 1673–159X(2021)03 − 0001 − 14

doi:10.12198/j.issn.1673 − 159X.3845

The Research Summary of the Development and Application of Blockchain Cross-chain Technology

HE Shuai, HUANG Xiangnian*, CHEN Xiaoliang
(*School of Computer and Software Engineering, Xihua University, Chengdu* 610039 *China*)

Abstract: After more than a decade of in-depth development, blockchain has formed a blockchain network with different characteristics and suitable for different application scenarios. Due to the isolation of blockchain and the high degree of isomerization between chains, the data flow and value transfer between blockchains have become the technical bottlenecks that hinder the widespread application of blockchain technology. The cross-chain technology of blockchain is an important technical means to realize the interconnection of blockchain and improve the interoperability and extensibility of blockchain. In view of the difficulty of cross-chain interaction between blockchains,the development and application of blockchain cross-chain technology are studied. The basic principles of cross-chain are explained, and the technical difficulties faced by cross-chain technology are analyzed. The current situation is emphasized. Finally, we summarized some cross-chain core technologies about the security risks and practical applications, and discussed the current challenges and future development directions of cross-chain technology.

收稿日期: 2020 − 12 − 02

基金项目: 国家自然科学基金项目(61902324)。

* **通信作者:** 黄襄念(1964—),男,教授,博士,硕士生导师,主要研究方向为模式识别。
ORCID: 0000 − 0003 − 3371 − 4379　　E-mail: huangxn@vip.qq.com

引用格式: 何帅,黄襄念,陈晓亮. 区块链跨链技术发展及应用研究综述[J]. 西华大学学报(自然科学版),2021,40(3):1 − 14.
HE Shuai, HUANG Xiangnian, CHEN Xiaoliang. The Research Summary of the Development and Application of Blockchain Cross-chain Technology[J]. Journal of Xihua University(Natural Science Edition), 2021, 40(3): 1 − 14.

Keywords: blockchain; cross-chain technology; interoperability; value transfer

比特币系统的成功稳定运行使得其底层区块链技术受到了广泛的研究与拓展。区块链技术也成为继物联网、大数据、云计算之后的又一项颠覆性前沿技术[1]。区块链技术涉及到了密码学、计算机科学、博弈论、数学等多个学科领域,是点对点网络、加密算法、共识机制、智能合约、分布式数据存储等多种技术的集成式创新[2],具有去中心化、不可篡改、可追溯、不可伪造的技术特点,实现了在开放式 P2P 网络中不依赖可信第三方的数字支付系统,正构造着全新的信任体系,有望实现信息互联向价值互联的转变,具有改变人类社会价值传递方式的潜力,支持与各行业应用深度融合,引起了金融、航运物流、电子政务等多个领域的广泛关注[2-3]。

区块链技术从诞生至今,历经了区块链 1.0 的比特币时代和以联盟链为代表的区块链 2.0 时代。经过近几年来区块链技术的深入创新发展以及区块链项目的不断落地,区块链技术过渡到了以 EOS 为代表的区块链 3.0 时代[4]。区块链是在比特币的基础架构之上不断革新拓展而来,目前根据节点的准入机制与去中心化程度可将区块链分为公有链、联盟链和私有链[5]。比特币在设计过程中并未充分考虑在更广泛范围应用时所需的图灵完备、安全性、可扩展性等需求,使得单个区块链很难解决所有技术问题,也不能广泛应用于其他实际场景,因此,催生了适用于不同行业范围的区块链项目[5-6]。例如 Linux 基金会在 2015 年发起了 Hyperledger 开源项目,旨在推动区块链的跨行业应用,其子项目 Fabric 经过多年的创新与发展更是受到了众多企业级公司的青睐,已经成为了联盟链项目开发的主流框架。在区块链项目呈现出百花齐放的态势的同时,随之而来的区块链互通性问题便成为了搭建区块链价值网络的技术瓶颈和核心问题[7]。

目前,各种区块链项目都是根据不同的实际应用场景和设计理念,采用不同的技术框架开发出的异构区块链,这使得大量区块链项目成为了一个个孤立的价值体系。随着区块链技术在供应链金融、供应链溯源等场景的深入应用,场景之间融合的需求越来越大,跨链之间的价值流通、应用协同需求日益显现。如何实现区块链之间的互联互通,建立一种高效、安全、通用性强的跨链技术体系,满足链与链之间的安全高效数据共享与业务协同成为了当前区块链研究的重中之重[8]。跨链技术将是推动区块链产业大范围快速落地运用的强力助推剂,更是区块链 3.0 时代的核心与关键技术。

1 跨链基础知识

1.1 跨链的产生

随着区块链网络的迅猛发展,各种区块链项目之间的融合需求日益增长,区块链技术对跨链交互的诉求越来越突出。区块链技术在交易处理能力和可扩展性方面始终限制着区块链大范围的落地应用。如何突破底层公链性能和功能瓶颈,实现高吞吐量和跨链互操作为一体的区块链系统成为了当前区块链领域研究的重点。在性能方面,区块链从单链逐渐发展为多链融合,通过对传统的工作量证明[9](proof of work, PoW)共识机制的改进和优化,在比特币和以太坊的基础架构上衍生出了以实用拜占庭容错[10](practical byzantine fault toleran, PBFT)和委任权益证明[11](delegated proof of stake, DPoS)共识算法为核心的联盟链和公链网络,实现了 TPS(服务器每秒处理的事务数)从个位数跃升到万级别的重大突破,但是在一定程度上弱化了区块链“去中心化”的核心设计理念;因此,在实际场景运用中区块链网络亟须在保证更好的去中心化前提下,实现更高的交易性能[12]。在功能方面,随着区块链技术深入研究与拓新、智能合约开发平台的逐渐丰富与优化完善,以及数字经济的快速发展,各种企业级商业区块链项目的落地实施使得大量纷繁复杂的垂直公链形成了众多独立的基础设施和业务体系[13]。为了实现不同行业区块链项目的有机融合,达到区块链间的互联互通,进而实现业务与价值的链间流转的目的,区块链对跨链交互技术有了实际的迫切需求,因此,跨链技术随之产生。

1.2　跨链的发展

跨链技术从比特币诞生之初就被初步的研究,经历了从单链扩张到中继等跨链平台的多链协同时期[14]。在区块链技术发展早期阶段,区块链技术都是基于单链的形式发展,但由于单链的性能优化和技术升级存在较大难度,不能满足实际应用需求;因此,大量基于单链扩张被研究,并逐渐过渡到了多链协同发展阶段[15]。2012 年瑞波实验室提出了 InterLedger[16] 协议,解决了区块链跨系统之间的协同问题;2013 年 Herlihy 提出了原子交换的理念,指出在构成一笔完整跨链交易的子交易中只存在 2 种情况,即成功和彻底失败[17];2014 年 BlockSream 提出了侧链机制,通过利用双向锚定实现了加密资产在主链与侧链之间的转移,并在此基础上提出了强联邦侧链,这不仅提升了互操作性,还有效地缩减了主链与侧链之间的时延;2015 年比特币闪电网络利用哈希时间锁定机制,实现了比特币链下快速交易,提升了比特币系统的交易效率;2016 年 BTC-Relay 利用中继跨链实现了比特币和以太坊之间的单向跨链通信;2017 年,在 Cosmos[16] 和 Polkadot[17] 跨链项目中提出了搭建跨链基础平台的方案,以实现兼容所有区块链应用的目的;2018 年 Wanchain 创世块降临[18],其在以太坊的所有机制之上引入跨链的交易机制,实现了链上资产的匿名性及隐私保护的功能;同年 7 月,Plasma 更新升级[19],在原有的基础之上简化了其功能设计,使得更新后的 Plasma 更加容易、费用更低;2019 年 Cosmos 上线,并利用 Cosmos-SDK 重构区块链生态系统,通过 Cosmos Hub[18－19] 将 Cosmos Networks 上的所有区块链连接起来共同创建了一个用于连接的中心核轮辐模型;同年,趣链跨链技术平台 BixXHub 和微众银行跨链平台 WeCross 开源,大力促进了着手打造国产自主的跨链技术平台的发展,专注于异构联盟链间的账本互操作,解决了跨链中的交易捕获、传输及验证的核心难题[19];2020 年 Polkadot 正式上线[20],其提供的互操作性和跨链通信实现了用户能够在链之间传递信息,打开了区块链创新服务的大门。

跨链技术从产生、发展到实际应用的过程中,在解决区块链互操作性、交易性和可扩展性方面都取得了一定的突破。目前,研究者正围绕着命名协议、身份认证与通信协议、跨链事务一致性等方面进行广泛的探索与研究。跨链技术发展历程如图 1 所示。

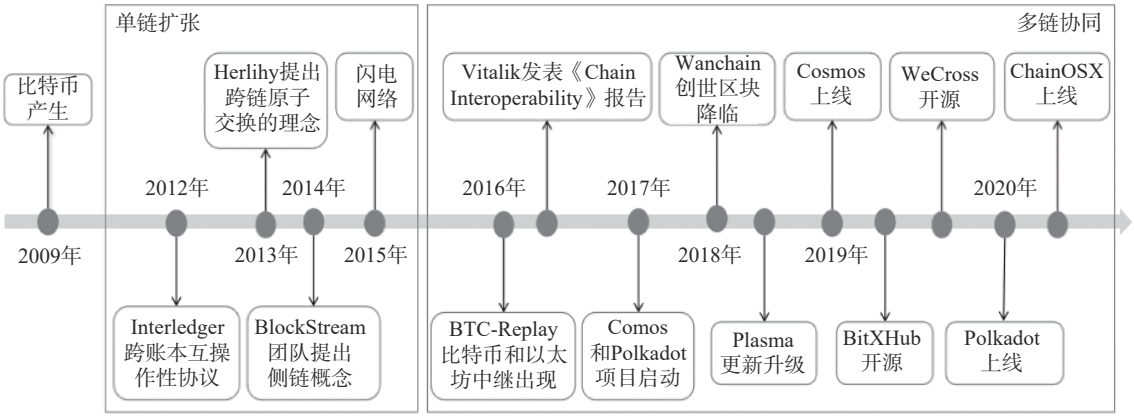

图 1　区块链跨链技术发展过程

1.3　跨链的原理

跨链,顾名思义,就是通过某些特定的技术手段,能让价值跨过链与链之间的障碍进行直接交互,从而实现不同区块链之间的资产流通和价值转移。跨链的实现原理和现实生活中货币兑换的原理是一致的,即通过既定的合法合规的准则达到不同区块链间的资产转移的目的。从商业应用的角度来看,跨链技术就相当于一个可信第三方交易所,不同的用户均可通过该交易所进行跨链交易,并且在跨链过程中并不会改变任意区块链上的价值总额,只是完成了不同区块链用户之间的价值兑换。跨链技术相对于传统的 TCP/IP 传输协议而言,有效地解决了账本之间在同步数据的过程中容易造成价值丢失和双重支付的问题。因此,跨链不

仅实现了信息的传输,还保证了在价值守恒的前提下,实现价值在不同区块链之间的流动[20]。总而言之,跨链技术是链接区块链的桥梁和枢纽,是实现价值互联的关键,是区块链向外拓展并打破区块链形成价值孤岛的有利手段。

1.4 跨链的类型

跨链交互根据所跨越的区块链底层技术平台的不同可以分为同构链跨链和异构链跨链。同构链之间的网络拓扑、安全机制、共识算法、区块生成验证逻辑都是一致的,因此同构链之间的跨链交互相对简单[19-21]。然而,在实际应用场景中,更多的研究是异构链之间跨链交互。异构链之间的共识机制、网络拓扑存在较大差异,使得异构链的跨链交互相对复杂。例如联盟链 Fabric 采用传统确定性共识算法,而比特币使用工作量证明(PoW)共识算法,导致了区块的确定性保证机制和组成形式产生了巨大差异,无法直接设计跨链交互机制而需要第三方服务辅助跨链交互,从而大大增加了异构链跨链交互的难度[22]。当前,不论是同构链跨链还是异构链跨链,要解决的最基础的问题还是链间资产的转移和资产的兑换[23]。在遵守跨链交易的原子性前提下,资产转移是指将原链上的资产进行锁定的同时在接受资产转移的目标链上重新铸造等值等量的资产,从而实现链之间的资产转移并实时更新各链上资产总量因转移而发生的变化[24];资产兑换是指在保证每条链上资产总量不变的情况下,同时变更交互链之间对链上资产的所有权,从而达到区块链间资产兑换的目的。目前,在异构链中跨链方式主要分为区块监听、不直接交互和第三方协作交互,其整体跨链架构如图 2 所示。

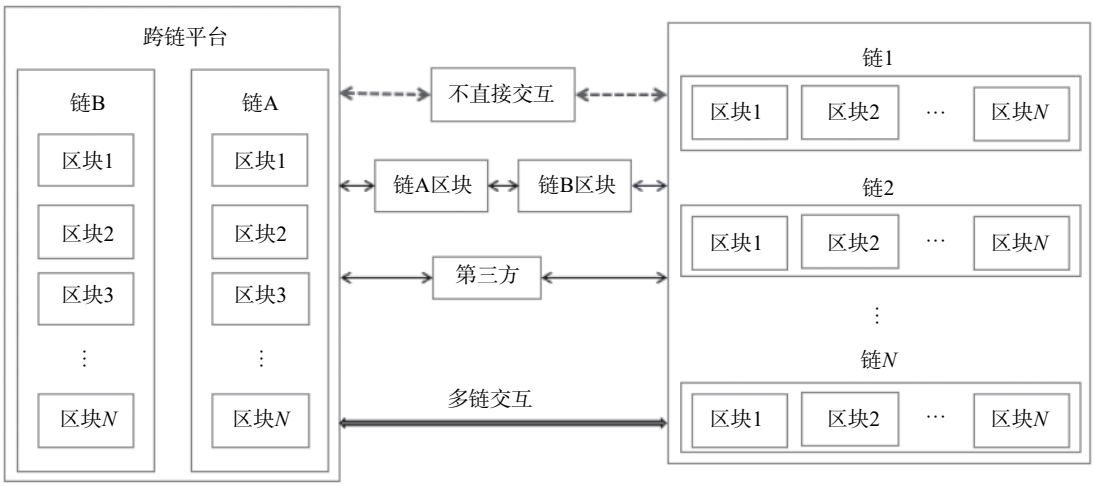

图 2 区块链整体跨链架构图

2 跨链技术的难点

随着大量区块链项目落地实施,为了促进区块链项目跨行业联合发展,解决区块链底层架构不同互通难、数据结构不同互认难、接口协议不同互联难、安全机制不同互信难、业务模式不同互访难等问题,跨链逐渐成为了当前区块链技术的重点攻关方向。由于跨链技术研究起点相对较晚,目前区块链的跨链技术研究仍处于萌芽阶段,正面临着各大风险挑战,跨链技术的创新研发也面临着各种各样的技术难点,主要体现在以下几个方面。

1)跨链事务管理问题。跨链技术在实现链间资产转移和兑换的过程中必须避免“双花”问题,即实现交易只能同时成功或同时失败,保证链间交易双方的账本信息同步更新且保持跨链事务的一致性。在一次跨链交易过程中往往包含多个子交易,这些子交易构成了一个事务,而不同的子交易通常独立并行地运行在不同的区块链系统中,跨链事务管理就必须保证在成功进行完一次交易后,其子交易也能够成功执行,如果某一子交易执行失败,则能够回滚撤销前面的子交易。因此,跨链事务管理在实现跨链交易的过程中要保证交易的原子性,这也是跨链技术必须要解决的技术难点。

2)跨链交易验证问题。跨链交易验证主要包括 2 方面:一是确认交易执行完成并成功写入区块

链账本;二是跨链交易双方在跨链交易过程中能够彼此验证交易的合法性和有效性。然而,在区块链系统中,为了确保信息的绝对可靠,大部分区块链系统是一个确定的、封闭的系统环境,这使得链内外的数据交互变得十分的困难,从而增加了验证另一条链中交易合法性和有效性的难度。目前“区块头+SPV”模式是常见的跨链交易验证机制[25]。

3)跨链交易性能问题。区块链的交易处理能力与可扩展性一直是区块链技术突破的重要方向。区块链系统在达成共识的过程中存在去中心化、安全性和可扩展性的不可能三角问题,使得区块链只能兼顾其中的 2 项[26]。尽管当前某些区块链项目能够达到数百万量级的 TPS,但都只有在少量验证节点的前提下才能实现,同时还降低了系统去中心化的特性。随着跨链交易规模的不断扩大,跨链交易对并发执行速度的性能需求越来越高,使得跨链交易并发性和可扩展性成为了跨链技术亟待解决的技术难点。

4)锁定资产管理问题。锁定资产管理能够实现链上资产锁定冻结,同时设定区块链上资产锁定和解锁的条件,能够有效地管理交易账户,确保锁定资产的私密性以及交易的安全性,也避免了交易过程中“双花”问题的出现。目前,锁定资产管理主要有智能合约模式、单一托管人模式以及联盟链托管模式。由于其应用场景和使用范围都有一定的局限性,因此跨链技术在锁定资产管理方面还有待进一步突破创新[23,26]。

5)多链协议适配问题。跨链技术是实现区块链技术达到真正的商业应用级别的助推剂。区块链网络要达到像互联网一样的互联平台,必须依靠跨链技术形成互联互通、多链互存的生态系统。目前,实现多链互联互通主要从主动兼容和被动兼容 2 个方向进行突破来解决多链协议适配问题。主动兼容是在已有的异构区块链系统基础之上,研发底层跨链机制,即从区块链的实际应用中开发适用于不同场景的跨链技术,进而实现跨场景的资产流通和价值转移。被动兼容是从底层平台入手,先搭建好跨链平台,在此基础上再进行区块链系统的开发,同时还可以提供接口接入更多的区块链系统,共享跨链平台的系统便利。

6)跨链安全保障问题。跨链的安全性问题是决定跨链网络能否正常运行的关键。区块链系统之间进行跨链交互时,如何确保双方系统的安全性是跨链技术研究一大难题。目前主要从适度隔离、检测安全事件 2 个方面进行考虑。适当隔离主要是为了避免当一条链受到攻击时影响整个跨链系统的运行,尽量保持链之间的独立性;检测安全事件是通过具有检测恶意攻击能力的第三方节点来处理跨链事务,使得跨链系统具有类似防火墙的功能。跨链安全保障问题将是跨链技术不断重视的一个技术研究点,也是跨链技术的防护盾,值得进一步深入研究并不断完善。

3　主流跨链机制

在业务形式日益复杂的商业应用场景下,链与链之间缺乏统一的互联互通机制,这将极大地限制区块链技术的发展空间。要实现真正的价值区块链网络,就必须将同构或异构的区块链网络连接起来。针对区块链之间的数据传输、交易访问等技术难点,目前已有公证人机制(notray scheme)、侧链/中继 (side chain/relay)、哈希锁定 (Hash-locking)、分布式私钥控制 (distributed private key control)、公证人+侧链混合机制 (notary scheme+sidechains mixing technology) 等[24,26] 核心技术在不同程度上解决了区块链跨链交互问题,实现了不同链之间资产自由流通。

3.1　公证人机制

公证人机制是一种相对容易实现的跨链机制。和传统的交易所工作模式类似,公证人机制是通过引入可信的第三方进行跨链消息的验证和转发。当在不同的区块链系统中进行资产兑换和转移时,选举一个或者多个组织作为公证人来自动或者请求式监听不同链上的事件,并通过特定共识算法对事件是否发生达成共识,最后及时做出响应[27]。目前,公证人机制根据实现过程中签名方式的差异又分为单签名公证人机制、多重签名公证人机制和分布式签名公证人机制。

3.1.1　单签名公证人

单签名公证人又称为中心化公证人,是公证人机制中最简单的跨链模式。其实质是指定单一的

独立节点或者机构充当公证人,该公证人在跨链交互过程中承担了数据收集、验证、交易确认的任务,并充当了冲突仲裁者的角色,进而实现了用可信第三方来替代技术上的信誉保障[28]。单签名公证人模式具有兼容性强、处理速度快的特性,但适用范围比较单一,大多数用于跨链资产兑换。基于单签名公证人模式的以太坊网络和比特币网络之间的资产交换过程如图 3 所示。

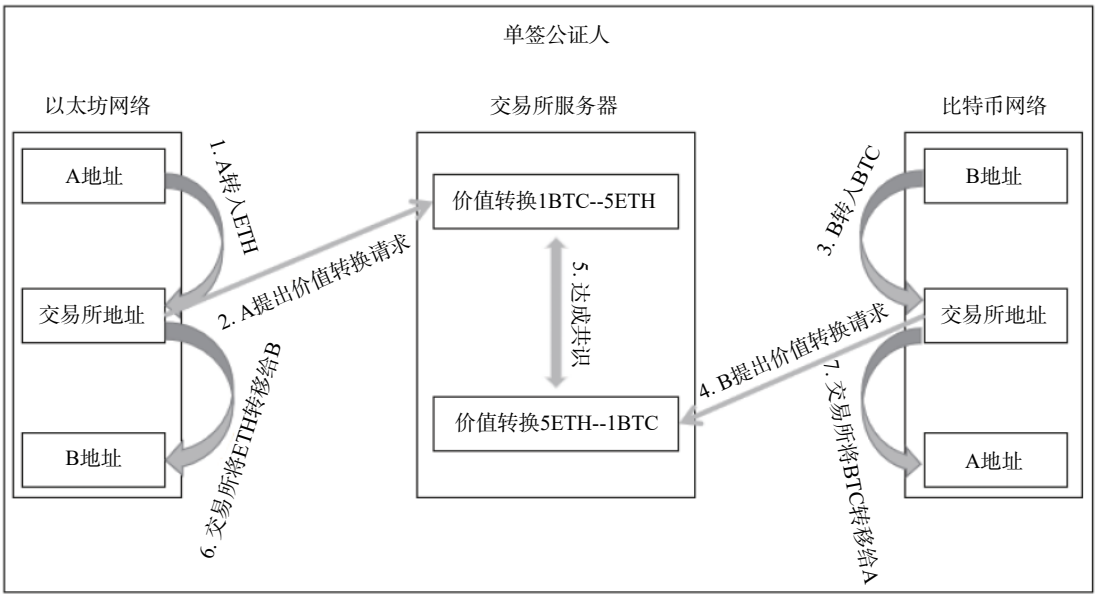

图 3 单签公证人跨链资产交换流程图

1)用户 A 将自己钱包地址里的 ETH 转入交易所地址账户中。

2)用户 A 向交易所提出价值兑换的请求:1BTC 兑换 5ETH。

3)用户 B 将自己钱包地址里的 BTC 转入交易所地址账户中。

4)用户 B 向交易所提出价值兑换的请求:5ETH 兑换 1BTC。

5)交易所作为可信第三方撮合交易双方达成共识。

6)交易所将用户 A 转入的 ETH 转移到用户 B 的钱包地址中。

7)同时交易所将用户 B 转入的 BTC 转移到用户 A 的钱包地址中。

3.1.2 多重签名公证人

多重签名公证人机制是在进行交易验证时从公证人群体中随机地选出一部分公证人,然后利用密码学技术来共同完成签名,降低了对公证人可靠性的依赖程度。在多重签名公证人模式中,公证人通常是一群独立节点或者机构组成的联盟,每一个节点都拥有一个密钥,只有当一定比例的公证人在各自的账本上共同签名达成共识时,跨链交易才能被确认[26-28]。相对于单签名公证人机制,多重签名公证人弱化了中心化风险,具有更高的安全性,当部分节点受到恶意攻击时不会影响整个跨链系统的运行。其实现过程如图 4 所示。

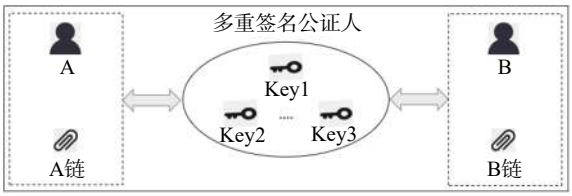

图 4 多重签名公证人流程图

3.1.3 分布式多重签名公证人

分布式签名公证人机制是在多重签名公证人机制上不断优化的具有更高安全性和可靠性的公证人跨链模式。相对于多重签名公证人机制而言,分布式签名公证人机制采用了多方计算 MPC(multi-party computation)的核心思想来确保密钥的隐私性和安全性[28-29]。分布式签名公证人模式的实现过程是将基于密码学生成的唯一密钥拆分成多个碎片,并将处理后的碎片随机分发给抽取的公证人,即使所有公证人将碎片拼凑在一起也无法得出密钥,只有当允许的一定比例的公证人共同完成签

名后才可拼凑出完整的密钥,从而实现更加去中心化的跨链交互[29]。其实现过程如图 5 所示。

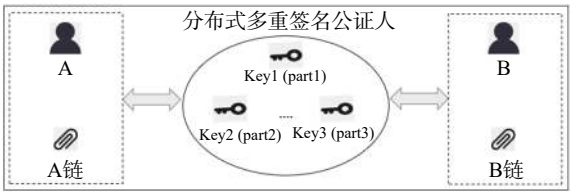

图 5　分布式多重签名公证人流程图

在公证人跨链模式中,Ripple 提出的 Interledger 协议[30](ILP)是最典型的公证人机制技术。ILP 不需要寻求任何形式的共识,它提供了一个称之为“连接者”的顶层加密托管系统。在这个中介机构的帮助下,不同区块链系统之间可以通过第三方“验证器”或“连接器”互相自由地传输数字资产[30－31]。

3.2　侧链/中继

侧链/中继(sidechains/relays)是一种能够自行检验交易数据且具有可扩展性的跨链技术。侧链和中继并没有严格的区分,从形式上看,侧链着重于表达链间的主从关系,中继是实现跨链的技术或方案。侧链是相对于主链而言的,主链不知道侧链的存在,但侧链知道主链的存在,当主链上需要处理较多的事务或者出现性能瓶颈时,可以将主链上的资产转移到侧链上处理,进而减轻主链上的压力,达到扩展主链功能和性能的目的。侧链实现的核心原理是双向挂钩技术。双向挂钩技术目前可以通过单一托管模式、联盟模式、SPV 模式、驱动链模式和混合模式来实现。中继是从各主链抽象分离出来的一个跨链操作层,提供了统一的语言,仅通过中间人收集 2 条链之间的数据状态进行自我验证,可减少链路之间通信的安全隐患,适用于链接 2 个异构或同构区块链[31]。由于中继跨链模式需要等待信息上链,因此其效率较低。

侧链和中继都是最常用的跨链模式,在实现过程中均需要采集原链上的信息,但两者在从属关系、执行过程、安全性方面也存在较大差异。在从属关系上,侧链从属于主链,主要侧重于优化区块链的可扩展性;中继没有从属关系,着重于跨链数据的传输。从执行过程看,由于侧链处理交易过程中需要同步所有的区块头,因此侧链的速度比中继慢[29,31]。在安全性方面,侧链和主链的安全性机制是独立的,由于侧链的安全性是建立在基于激励机制进行交易一致性验证的基础之上的,所以主链的安全性并不能在侧链上起作用;中继完全是由主链自行验证,因此具有更高的安全性能[32]。

侧链/中继跨链模式可以在链中创建智能合约,该智能合约将发起链的区块头为输入,使用发起链内的标准检验方式来检验区块链是否满足共识算法规范要求。侧链/中继以轻客户端验证技术为基础,即在跨链交互的过程中,在一条链上执行类似区块链轻客户端功能的智能合约,通过另一条链的加密哈希树以及区块头来验证链间的某项特定交易、事件或状态信息是否发生[31－32]。以太坊能做为比特币的侧链,并采用中继进行跨链交互,其实现过程如图 6 所示。

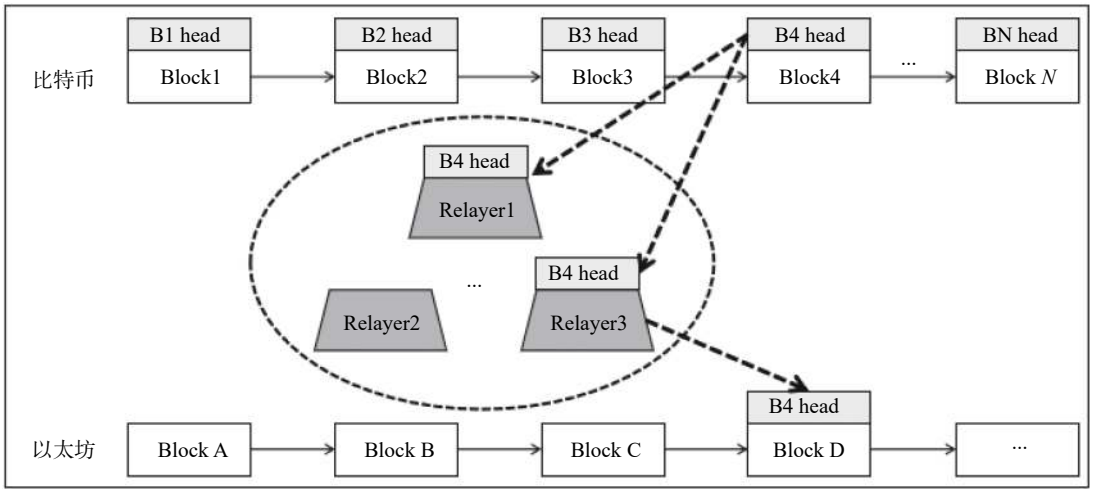

图 6　侧链/中继跨链交互流程图

3.3 哈希锁定

哈希锁定全称为哈希时间锁定合约(Hash timelock contract),是在无需可信公证人的情况下,通过哈希锁和时间锁共同完成链间资产兑换的一种跨链技术方案。在实现过程中,发起者首先随机选取秘密值作为哈希解密密钥,然后将秘密值进行哈希计算并将得到的哈希值作为哈希上锁的公钥发送给响应者;发起者和响应者将各自数字资产通过哈希值锁定在智能合约中,同时设置各自的时间锁(通常发起者的时间锁大于响应者的时间锁),如果在规定时间内双方都提供了秘密值,则合约中锁定的资产将兑换成功,否则,只要有任何一方不能在规定的时间内提供秘密值(哈希解密密钥),则合约中锁定的资产将被对方收回。哈希锁定的原子互换协议保证了同一条链中的资产总量保持不变,但哈希锁定的使用范围比较局限,通常只能用于跨链的资产兑换,并不能实现资产的跨链转移。最典型应用是利用哈希锁定实现 ETH 到 BTC 的原子交换,其实现过程如图 7 所示。

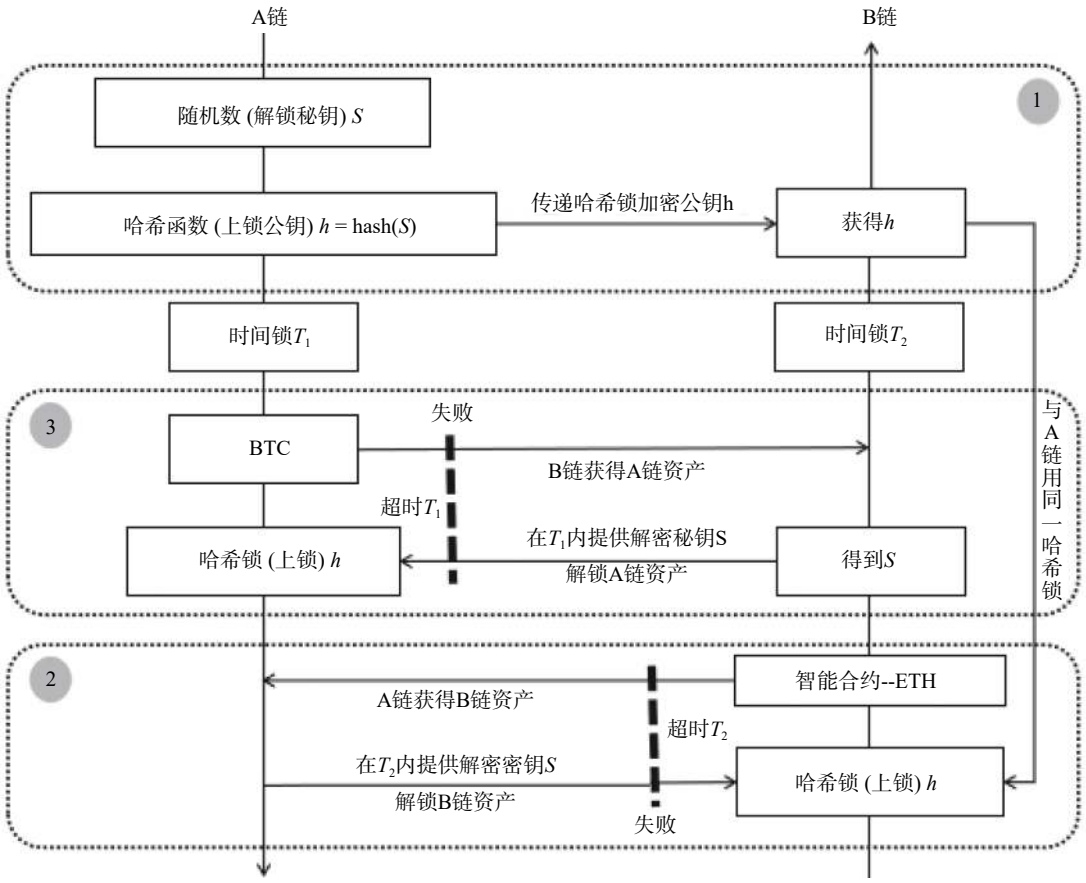

图 7 哈希锁定跨链交互流程图

1)A 链产生随机数 S,同时计算出对应的哈希值 h,并将 h 通过网络传递给 B 链。

2)在 A 链上设置时间锁,并通过哈希值 h 将 BTC 锁定在 A 链的智能合约中。

3)B 链设置时间锁,同时使用从 A 链传递过来的 h 将 ETH 锁定在 B 链的智能合约中。

4)A 链在时间 T_2 范围内向 B 链提供 S(解锁秘密值),B 链将锁定的 ETH 转移到 A 链,同时获得 S,超时则跨链失败,双方取回智能合约中的资产。

5)B 链在时间 T_1 范围内向 A 链提供 S(解锁秘密值),A 链将锁定的 BTC 转移到 B 链,超时则跨链失败,双方取回智能合约中的资产。

6)任何一条链未在对方时间锁规定的时间范围内提供 S 均会导致整个跨链资产兑换失败。

3.4 分布式私钥控制

分布式私钥控制(distributed private key control),顾名思义,就是采用分布式节点来控制区块链系统中各种资产的私钥,将数字资产的使用权和所有权

进行分离,使得对链上资产的控制权能安全地转移到非中心化系统中,同时将原链上的资产映射到跨链中,实现不同区块链系统间的资产流通和价值转移[33]。分布式私钥控制的实现过程是利用一个基于区块链协议的内置资产模板,根据跨链交易信息部署新的智能合约来创建出新的加密货币资产[26,33]。当一种已注册资产由原有链转移到跨链上时,跨链节点会为用户在已有合约中发放相应等值代币,确保了原有链资产在跨链上仍然可以相互交易流通。分布式私钥控制在 Fusion 区块链项目中得到了应用,其资产锁定(Lock-in)过程如图 8 所示。首先需要将密钥分片并生成分布式密钥,然后通过 Fusion 节点来验证转入原链上指定账户的资产,从而达到分布式管理控制权的目的[34]。具体步骤如下。

1)用户首先向 Fusion 发出锁定资产的请求。

2)Fusion 根据用户请求生成分布式密钥和锁定(Lock-in)资产的地址。

3)Fusion 将生成的 Lock-in 地址发送给用户,用户便可将资产转入地址中。

4)Fusion 锁定地址和对应的密钥并更新验证用户的资产。

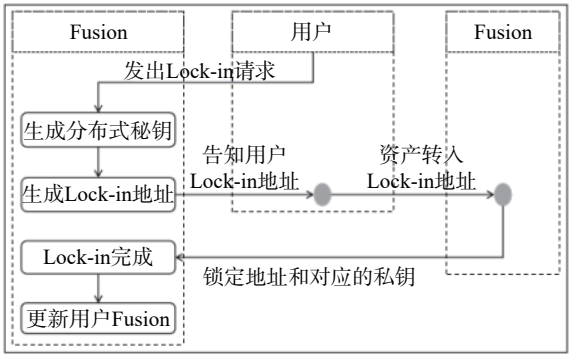

图 8　Fusion 中 Lock-in 过程示意图

3.5　公证人+侧链混合机制

在已有的 4 种主流跨链技术基础之上,研究者将具有实现简单、容易操作、双向跨链等优点的公证人机制和具有独立性、快速高效特性的侧链相结合,提出了公证人+侧链混合技术 (notary scheme+sidechains mixing technology) 来提高跨链交互性能,并在实际场景中得到了应用。公证人+侧链混合技术充分发挥了 2 种机制的优势,通过侧链技术提高区块链系统间高效通信的效率,利用公证人机制实现资产跨链,进而支持跨链资产交互、跨链合约以及资产抵押,实现了由分布式节点做公众,避免了中心化的控制,是链与链之间互操作最简单的方法。其在提高跨链交互效率的同时,区块链之间使用共同信任的分布式节点充当公证人完成资产交换,实现跨链交互。目前,Ether Universe 是世界首个采用公证人机制+侧链混合技术实现基于第 3 代区块链平台 EOS.IO 构建的跨链服务平台,是一套完全创新的跨链交互技术解决方案[35]。

3.6　跨链技术性能分析及比较

目前,虽然已有的 5 种主流的跨链机制在不同程度上解决了跨链存在的各种问题,在某些技术瓶颈上也取得了一定的性能提升,但由于它们的实现原理和针对的应用场景不同;因此,现有的跨链技术都存在较大的局限性。为更加全面直观地了解 5 种主流跨链之间的差异,本文从互操作性、信任模型、交易处理、多币种智能合约、技术安全与性能等方面进行了分析及比较,如表 1 所示。

从对比结果来看:在互操作性方面,哈希锁定是一种交叉依赖关系,相对于其他几种跨链模型存在明显的不足;在信任模型方面,公证人机制需要多处可信第三方作为公证人,容易造成中心化,而其他几种跨链模型不存在这方面问题;在跨链交易处理方面,哈希锁定的局限性比较大,大多数情况下能支持跨链资产抵押,但不支持跨链资产转移,也不直接支持跨链原语操作,而其他几种跨链模式都能较好地支持跨链交易的相关操作;在多币种智能合约方面,只有分布式私钥控制技术能够得到有效的支持,其他几种跨链模式都还有待优化完善;在技术安全与性能方面,公证人模式、侧链/中继模式的安全性都比较低,交易速度也还有待提升,公证人+侧链混合模型在安全性和交易速度方面都较好,但实现难度较高。总之,目前还没有一套完整的适用于任何场景的跨链标准和体系,在不同的应用背景下,需要全方位的考虑跨链技术本身的条件和存在的问题,选择合适的跨链模型解决相应的实际问题。

4　跨链技术应用及安全性分析

4.1　跨链技术的应用

跨链技术研究取得的成果,已经在跨链体系结构、跨链数据协同、跨链资产流通等方面开展了相关的实践应用,并在分布式交易、数字金融创新等

表 1 跨链机制性能对比分析

比较项目	区块链主流跨链机制				
	公证人机制	侧链/中继机制	哈希锁定机制	分布式私钥控制机制	公证人+侧链混合机制
互操作性	所有	所有	交叉依赖	所有	所有
信任模型	多数公证人诚实	链不会失效	链不会失效	链不会失效	混合模式
跨链交易	支持	支持	支持	支持	支持
参与链数量	多链	双链/多链	双链	多链	双链/多链
跨链资产转移	支持	支持	不支持	支持	支持
跨链资产抵押	支持	支持	大多数支持	支持	支持
适用跨链原语	支持	支持	不直接支持	支持	支持
多币种智能合约	困难	困难	不支持	支持	困难
费率	中	高	中	中	低
安全性	低	低	中	中	高
交易速度	慢	慢	中	中	快
实现难度	中等	较难	容易	中等	较难
局限性	依赖第三方公证人	适应场景多、接入链绝对一致性	场景单一、发起人掌握主动权	应用范围小、智能合约待完善	实现多币种智能合约困难
典型案例	Ripple	RootStock/Cosmos	Lighting Network	Fusion/Wanchain	Ether Universe

领域取得了一定的进展。众享比特使用 Ripple 提出的跨链价值传输的技术协议 InterLedger Protocol, 实现了跨链资产转移[36]; Plasma 设计的区块链树形框架通过了智能合约激励执行与强制执行[37]; MIT 的 Thomas 等提出的一套跨链设计理念在 Tradecoin 中进行了实践[37]; ConsenSys 提出的 BTC Relay, 使用侧链技术实现了区块链间资产流通[38]; Cosmos 建立 Tendermint 开发框架, 推出了 Cosmos Hub[39]; Polkadot 使用中继链建立了一个可伸缩的异构多链系统[40]。

国内对跨链技术的研究与应用也投入了大量的人力、物力, 提出了广泛先进的科研平台。华中科技大学的金海教授提出了一种支持多链互操作的分层架构[41]; 上海软件中心提出一种跨链公证人评价模型, 对收集到的公证人节点信息进行信用计算, 保证跨链系统的安全稳定, 同时联合复旦大学、同济大学、万向区块链等研发了区块链跨链操作系统 ChainOSX[42]; 微众银行自研的跨链平台 WeCross, 满足同构区块链平行扩展后的可信数据交换需求[43]; 趣链科技构建了支持同构及异构区块链间交易的跨链技术示范平台 BitXHub[44]。总之, 跨链技术正迎来研究热潮, 跨链技术的实际运用将呈现井喷式增长。部分典型跨链研究机构的项目成果及应用情况如表 2 所示。

表 2 跨链部分研究成果及应用情况

机构名称	研究内容	研究成果	应用情况
Ripple公司	不同支付网络或账本交互	Interledger	应用于不同分类账之间的安全转账场景
Tendermint公司	中继链验证节点共识(DPoS+BFT)	Cosmos	异构链间资产交互
Tendermint团队	支持跨链交互的异构网络	Cosmos	应用于跨链交易场景
R3CEV公司	公证人模式跨链技术	Croda	基于公证人模式的分布式账本
Polkadot团队	支持多种链结构的异构多链跨链平台	Polkadot	主要以以太坊为主, 实现与其他私链互连
Fusion公司	分布式控制权限管理跨链技术	Fusion	应用于去中心化签名跨链交易
网录科技	安全多方计算+门限密钥	Wanchain	资产交互、数据互通
微众银行	分布式商业区块链跨链协作	WeCross	应用于物联网跨平台联动、数字资产交换
趣链科技	支持同构及异构区块链间的跨链交易	BitXHub	用于异构链的资产交换及信息互通

目前,在 5 种主流的跨链机制基础上,针对不同的区块链平台研发出了大量的跨链前沿技术,并在一定程度上解决了区块链系统内部和系统间的跨链问题,极大地促进了区块链技术的应用发展。根据区块链平台的差别,跨链技术主要可以分为基于 BTC 区块链的跨链技术、基于 ETH 区块链的跨链技术以及自有链跨链技术。

基于 BTC 区块链的跨链技术是指在 BTC 基础上通过开发属于 BTC 区块链的侧链等方法来解决 BTC 区块链容量限制及交易手续费高的问题,例如 Pegged Sidechains 与闪电网络等技术[45]。基于 ETH 区块链的跨链技术是指在 ETH 基础上,为了解决 ETH 区块链的可扩展性不足、性能低下、资源不隔离等问题研发的一系列跨链技术,例如 Plasma Cashh 和 Loom 等[46]。自有链跨链技术是针对整个区块链生态,着力于构建具有跨链特性的区块链项目,并致力于寻求现实通用的、标准化的区块链接入模型[47]。

随着区块链技术在各个行业领域的应用与创新,跨链技术作为连接不同区块链的枢纽,已经得到了业界广泛的认可。根据跨链技术的作用范围(系统内部/系统间)、跨链机制类型(公证人/侧链(中继)/哈希锁定/通信协议族)以及区块链平台(基于 BTC/ETH/自有链),本文对当前已有的跨链技术或项目进行了总结,如表 3 所示。从现有技术来看:跨链技术主要针对不同区块链系统间的跨链交互展开;在公链中,基于 BTC 和 ETH 区块链的跨链项目数相当,表明这二者在公链中对跨链具有广泛的应用基础和更迫切的需求[48],同时,自有链类型的跨链技术也在不断创新发展。力求研发一套通用的、完整的、标准的跨链体系,是区块链跨链技术未来需要不断突破的方向和发展趋势。

表 3　跨链技术汇总

跨链技术名称	区块链平台类型	跨链机制类型	跨链作用范围
Pegged Sidechains	基于BTC区块链	侧链	系统间
Lightning Network	基于BTC区块链	哈希锁定	系统间
RootStock	基于BTC区块链	侧链	系统间
Elements	基于BTC区块链	侧链	系统间
Factom	基于BTC区块链	–	系统间
BTC-Relay	基于ETC区块链	侧链	系统间
Sharding	基于ETC区块链	–	系统内部
Plasma	基于ETC区块链	侧链	系统间
Minimal Viable Plasma	基于ETC区块链	侧链	系统间
Plasma Cash	基于ETC区块链	侧链	系统间
Loom	基于ETC区块链	侧链	系统间
Bancor	基于ETC区块链	–	系统间
Interledger	自有链	公证人、哈希锁定	系统间
Cosmos	自有链	中继、通信协议族	系统间
Polkadot	自有链	中继	系统间
Lisk	自有链	侧链	系统间
Aion	自有链	通信协议族	系统间
Nano	自有链	–	系统内部
Zcash XCAT	自有链	哈希锁定	系统间
OneLedger	自有链	通信协议族	系统间
Wecross	自有链	通信协议族	系统间
BitXHub	自有链	侧链、中继	系统间

4.2　跨链安全性分析

跨链技术是针对区块链跨链交互需求而提出的,因此跨链技术的健壮性必将与区块链在实际应用中所面临的各种安全性问题息息相关,跨链技术的发展也将与区块链技术的应用模式密不可分。区块链技术多样性的发展将会对跨链技术提出更高的要求,然而目前支持跨链数据通信的各类跨链协议大部分处于研发状态,暂未获得广泛的认可和共识。因此,对区块链常见的安全性问题进行分析,有利于完善跨链技术在安全性方面存在的漏洞。

1)阻塞超时。区块链系统间在进行跨链交易的过程中,为了确保交易的原子性以及避免孤块问题,通常会设置交易的延迟时间以促使交互数据能够在区块链上得到有效的确认。由于当前区块链系统的 TPS 较小,交易速度慢,并发处理事务的能力低,因此区块链网络常常出现阻塞和超时的问题。例如在比特币系统中,如果多次交易阻塞超过几小时甚至数天未被确认,将会引起大面积跨链交易超时阻塞的风险。

2)日蚀攻击。区块链在实现过程中为达到去中心化的目的,需要以高效的共识机制和 P2P 网络为基础,但由于当前 TCP 协议的局限性,P2P 网络单个节点连接到其他节点的数量非常有限;因此,攻击者可以通过囤积和霸占受害者点对点连接的

间隙,进而屏蔽受害者所有的输入和输出节点,从而阻止最新的区块链信息进入日蚀节点,最终达到隔离节点的目的。

3)长距离攻击。长距离攻击往往出现在基于权益证明(PoS)共识机制的区块链网络中。在基于工作量证明(PoW)共识机制的比特币系统中,长距离攻击是指要想具有篡改账本的能力,攻击者至少必须要控制 51% 的算力,在 P2P 网络中难以实现,然而由于 PoS 缺乏对算力的约束,恶意节点能够导致原始区块链出现重组;因此,账本被篡改的风险将大大提升。目前可以通过设立确定性检查点来预防此类攻击。

4)竞争条件攻击。原子交换类的跨链系统通常对交易确认的先后性存在差异,即参与交易的任何一方均有可能被先确认,从而导致竞争条件攻击。例如交易双方希望通过跨链系统提供的智能合约实现 BTC 和 ETH 之间的兑换,发起方和接收方分别将 BTC 和等值的 ETH 发送到合约指定的地址中,这时接收方可以再向智能合约指定的地址中转入与发起方相同的 BTC,如果接收方的交易先被确认,那么接收方就能取回自己转入合约地址中的 ETH,同时得到发起方转入合约地址的 BTC,而发起方一无所获,从而达到竞争条件攻击的目的。

5)跨链重放攻击。区块链网络中的节点在争夺记账权的时候容易出现硬分叉,导致区块链发生永久性分歧并产生 2 条或多条交易历史、交易地址、交易格式、密钥算法以及余额完全相同的链,使得一条链上的交易有可能被恶意传送到其他链上重新广播而得到确认[49]。比较典型的重放攻击是在以太坊硬分叉中出现 ETH 和 ETC 2 条链,导致交易者从交易所提取 ETH 币时有可能得到同等数量的 ETC 币,从而造成资产的损失。

此外,区块链系统在共识机制方面还存在币龄累计攻击、预计算攻击、女巫攻击;在分布式网络中还存在窃听攻击、分割攻击、双重支付攻击;在加密签名机制方面还存在穷举攻击、碰撞攻击、长度扩展攻击、后门攻击、量子攻击;针对区块链数据还有恶意信息攻击、资源滥用攻击等[50]。总之,区块链所面临的安全性问题在跨链系统中将变得更加复杂。因此,在跨链系统的设计过程中需要引入保护机制,同时全方位充分了解区块链技术亟待解决的安全性问题,才能促使跨链技术向着更加健全的方向发展。

5 跨链技术的挑战与前景

跨链技术已经成为实现链联网和构建价值网络高速公路的核心关键技术,是推动区块链产业跨场景融合发展的科技引擎。随着区块链技术的持续探索,未来必将形成多链互连共生的区块链生态圈,区块链的多样性也必将导致对跨链技术更迭的要求不断提高,对跨链的需求也必定不再局限于交易。在未来,随着区块链技术的应用不断普及,着力研发类似于互联网中标准化的数据接口通信技术,构建链连网,实现各种区块链间的跨链交互是跨链技术的发展趋势。

5.1 跨链技术面临的挑战

当前各类区块链系统最大的问题就是缺乏互操作性,因此跨链技术要着力解决如何适配各类区块链,并确保跨链操作的高效率性和高安全性。跨链技术实现难度较大,目前仍处于初步探索的阶段,还尚未形成统一的跨链标准和稳定的跨链体系。在未来的发展过程中必然还会遇到各种挑战,要实现真正的价值互联,让区块链系统能够像现在的操作系统对互联网 TCP/IP 协议的支持一样得到大范围落地应用,还有大量的问题亟待解决。例如跨链网络之间的安全性问题和连接健壮性问题、跨链网络之间恶意行为的预警和制止问题、跨链网络激励制度的优化问题、跨链交易中目的链的死循环问题、母链分叉问题等[49-50],都是跨链技术在发展过程中不得不面临的挑战。

5.2 跨链技术的发展前景

近几年来,区块链技术的热度居高不下,世界多个国家已经将区块链上升至国家战略层高度,争先抢占区块链创新发展制高点。在当前区块链应用场景需求日益激增和政府大力扶持的情况下,我国已将区块链作为国家新基建信息基础设施的重要组成部分。跨链技术也必将伴随着区块链技术的深入探索得到不断创新与发展。当下,跨链技术正迎来新一轮的研究热潮,在未来必将围绕跨链体系结构的多链协议互通性、跨链数据传递验证的

安全可信性、跨链交易及合约执行的一致性、跨链系统接入及治理的高效性等方面展开广泛而深入的研究与探索,将一步步突破新一代互联、可信和高效的技术瓶颈,支持跨场景、跨地域的应用,实现跨区块链互通和协同,塑造更具前景和活力的商业模式,开启万链互联的时代。

参　考　文　献

[1] 张亮, 刘百祥, 张如意, 等. 区块链技术综述[J]. 计算机工程, 2019, 45(5): 1 − 12.

[2] 蔡晓晴, 邓尧, 张亮, 等. 区块链原理及其核心技术[J]. 计算机学报, 2021, 44(1): 84 − 131.

[3] 何蒲, 于戈, 张岩峰, 等. 区块链技术与应用前瞻综述[J]. 计算机科学, 2017, 44(4): 1 − 7.

[4] 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.

[5] SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969 − 988.

[6] 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.

[7] 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.

[8] 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.

[9] 江鹏. 跨链技术概览及项目对比 [EB/OL]. [2020-10-06]. http://www.mimajike.com/2417/.html.

[10] KWON J, BUCHMAN E. Cosmos: A network of distributed ledgers[EB/OL]. [2020-10-06]. https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md.

[11] HERLIHY M. 原子跨链交换 [C]//2018ACM 分布式计算原理研讨会的研讨会. San Francisco: ACM, 2018: 245 − 254.

[12] HOPE-BAILIE A, THOMAS S. Interledger: creating creating a standard for payments[C]//Proceedings of the 25th International Conference Companion on World Wide Web. Canada: [s.n.], 2016: 281 − 282.

[13] 喻辉, 张宗洋, 刘 建 伟. 比特币区块链扩容技术研究[J]. 计算机研究与发展, 2017, 54(10): 2390 − 2403.

[14] 魏昂. 一种改进的区块链跨链技术[J]. 网络空间安全, 2019, 10(6): 40 − 45.

[15] 徐卓嫣, 周轩. 跨链技术发展综述[J]. 计算机应用研究, 2020, 38(2): 341 − 346.

[16] KWON J, BUCHMAN E.Cosmos whitepaper [EB/OL].[2020-10-08]. https://cosmos.network/resources/whitepaper.

[17] NOLAN T. Alt chains and atomic transfers [EB/OL]. [2020-10-06]. https://bitcointalk.org/index.php?topic=193281.0.

[18] WANCHAIN Ltd. System and method for universal blockchain interoperability: USPTO 20200278958[P]. 2020.

[19] BUTERIN V. Minimum viable plasma [EB/OL]. [2020-10-08]. https://ethresear.ch/t/minimal-viable-plasma/426.

[20] GAVIN W. Polkadot:vision for a heterogeneous multi-chain framework[EB/OL].[2020-10-08].https://polkadot.network/Polkadot-lightpaper.pdf.

[21] 吕旭军, Dustin Byington. 万维链: 区块链跨链技术及应用生态[J]. 杭州(周刊), 2018(18): 32 − 33.

[22] BUTERIN V. Chain interoperability[EB/OL]. [2020-10-06]. https://www.r3.com/download/chain-interoperability.

[23] 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.

[24] 郭朝, 郭帅印, 张胜利, 等. 区块链跨链技术分析[J]. 物联网学报, 2020, 4(2): 35 − 48.

[25] 俞学劢. 基于 SimpleChain Beta 的跨链交互与持续稳态思考[J]. 信息化建设, 2019(11): 54 − 56.

[26] 赵涛, 张凌浩, 赵其刚, 等. 基于聚类簇中心的共识跨链交换模型[J]. 计算机科学, 2019, 46(S2): 557 − 561.

[27] 顾小力. 当前区块链技术的研究进展及发展前景[J]. 信息与电脑(理论版), 2018(16): 106 − 107.

[28] NAKAMOTO S. Bitcoin: A Peer-to-peer electronic cash system[EB/OL]. [2020-10-06]. https://bitcoin.org/en/bitcoin-paper, 2019-4-9.

[29] MARK F. Compact SPV proofs via block header commitments[EB/OL]. [2020-10-06]. http://sourceforge.net/p/bitcoin/mailman/message/32111357/, 2019-4-15.

[30] 邵奇峰,金澈清,张召,等. 区块链技术:架构及进展[J]. 计算机学报, 2018, 41(5): 969 − 988.

[31] MENDLING J, WEBER I, AALST W V D, et al. Blockchains for business process management-challenges and opportunities[J]. ACM Transactions on Management Information Systems (TMIS), 2018, 9(1): 4.

[32] 陈伟利, 郑子彬. 区块链数据分析: 现状、趋势与挑战[J]. 计算机研究与发展, 2018, 55(9): 1853 − 1870.

[33] 王皓, 宋祥福, 柯俊明, 等. 数字货币中的区块链及其隐私保护机制[J]. 信息网络安全, 2017, 17(7): 32 − 39.

[34] 孙毅, 范灵俊, 洪学海. 区块链技术发展及应用: 现状与挑战[J]. 中国工程科学, 2018, 20(2): 27 − 40.

[35] 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.

[36] 于鸿源, 叶雄兵, 张立韬, 等. 基于 Ripple 共识机制的分布式作战资源分配方法研究[J]. 信息工程大学学报, 2019, 20(6): 750 − 757.

[37] 刘桂华. 基于公证人组的区块链跨链机制 [D]. 重庆: 重庆邮电大学, 2020.

[38] Ethereum. Welcome to BTC relay's documentation[EB/OL].[2020-09-18]. https://btc-relay.readthedocs.io/en/latest/.

[39] 吴晓晖, 黄昌军, 吴梦蝶, 等. 区块链技术在访问控制的研究进展[J]. 科技风, 2020(35): 102 − 103.

[40] 贺海武, 延安, 陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展, 2018, 55(11): 2452 − 2466.

[41] LEMAHIEU C. Nano: A feeless distributed cryptocurrency network[EB/OL]. [2020-10-06]. https://nano.org/en/whitepaper.

[42] THOMAS S, SCHWARTZ E. A protocol for interledger payments[EB/OL]. (2020-08-03). https://interledger.org/interledger.pdf.

[43] DEICHLER A. Interoperability: the holy grail of blockchain[EB/OL]. (2017-10-25). https://www.afponline.org/ideas-inspiration/to-pics/articles/Details/interoperability-the-holy-grail-of-blockchain.

[44] 刘权. 区块链与人工智能 构建智能化数字经济世界 [M]. 北京: 人民邮电出版社, 2019.

[45] WOOD G. Polkadot: Vision for a heterogeneous multi-chain framework[EB/OL]. [2020-10-06]. https://github.com/polkadot-io/polkadotpaper/raw/master/PolkaDotPaper.pdf.

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

[47] 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.

[48] 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.

[49] 韩璇, 袁勇, 王飞跃. 区块链安全问题: 研究现状与展望[J]. 自动化学报, 2019, 45(1): 206 − 225.

[50] OneLedger. A universal blockchain protocol enabling cross-ledger access through business modularization[EB/OL].[2020-10-06].https://oneledger.io/wpcontent/uploads/2018/04/oneledger-whitepaper.pdf.

(编校: 饶莉)