doi :10.3969/j.issn.1671-1122.2019.08.012

区块链跨链技术研究

路爱同，赵阔，杨晶莹，王峰

（吉林大学计算机科学与技术学院，吉林长春 130012）

摘　要：随着区块链技术的持续发展和创新，支付结算、产品溯源、身份认证等领域出现了具有不同特点、适应不同场景需求的大量区块链网络，形成了诸多价值孤岛。区块链跨链技术是实现链间互联互通和价值转移的重要技术手段。文章对目前区块链主流跨链技术进行了系统总结，首先介绍了跨链技术特性，然后介绍了跨链技术的难点及其参考解决方案，接着介绍了 4 种主要的跨链技术，最后分析了跨链技术面临的挑战并对其未来进行了展望。

关键词：区块链；跨链；互操作性

中图分类号：TP309　**文献标识码：**A　**文章编号：**1671-1122（2019）08-0083-08

中文引用格式：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·

英文引用格式：LU Aitong, ZHAO Kuo, YANG Jingying, et al· Research on Cross-chain Technology of Blockchain[J]· Netinfo Security, 2019, 19(8): 83–90·

Research on Cross-chain Technology of Blockchain

LU Aitong, ZHAO Kuo, YANG Jingying, WANG Feng

(*College of Computer Science and Technology, Jilin University, Changchun Jilin* 130012 *China*)

Abstract: With the continuous development and innovation of blockchain technology, a large number of blockchain networks with different characteristics and adapting to different scenarios have emerged in the fields of payment and settlement, product traceability and identity authentication, forming many value islands· Blockchain cross-chain technology is an important technical means to achieve inter-chain connectivity and value transfer· This paper systematically summarizes the current mainstream cross-chain technologies· Firstly, this paper analyzes the characteristics of cross-chain technology, and then summarizes the difficulties of cross-chain technology and its reference solutions· Furthermore, this paper introduces four main cross-chain techniques· Finally, this paper analyzes the challenges of cross-chain technology and forecasts its future prospect·

Key words: blockchain; cross-chain; interoperability

收稿日期：2019-5-16

基金项目：国家重点研发计划 [2017YFA0604500]；国家自然科学基金 [61701190]；吉林省中青年科技创新领军人才及团队项目 [20170519017JH]；吉林省青年科学基金 [20180520021JH]；吉林省重点科技研发项目 [20180201103GX]；中国博士后科学基金 [2018M631873]；吉林省发展与改革委员会项目 [2019FGWTZC001]

作者简介：路爱同（1992—），男，山东，硕士研究生，主要研究方向为区块链；赵阔（1977—），男，吉林，副教授，博士，主要研究方向为网络空间安全、大数据处理技术、云计算、物联网、区块链；杨晶莹（1996—），女，吉林，硕士研究生，主要研究方向为区块链；王峰（1987—），男，吉林，副教授，博士，主要研究方向为网络空间安全、物联网、数据融合。

通信作者：赵阔 zhaokuo@jlu.edu.cn

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

0 引言

区块链[1]技术源自化名为“中本聪（Satoshi Nakamoto）”的学者在2008年10月31日发表的奠基性论文“Bitcoin: A Peer-to-Peer Electronic Cash System”。区块链是一种集成式创新，涉及的技术包括对等（P2P）网络、拜占庭容错[2]、智能合约以及分布式共识算法等[3]，真正地在开放式P2P网络中实现了不依赖于可信第三方的数字支付系统，具有去中心化、去信任化、不可篡改和可追溯等优点。这对于传统社会组织和运作方式是一种颠覆性的变革和挑战，被认为是构建未来“信任互联网”“价值互联网”的支撑性技术，受到了投资界、学术界、工业界及政府部门等的越来越多的关注[4]。

自2008年起，以比特币为代表的区块链1·0时代和以以太坊（Ethereum）[5]和联盟链为代表的区块链2·0时代都取得了突破性的进展。2009年1月4日，比特币创世区块诞生。2013年，BUTERIN[6]提出以太坊的概念并写下《以太坊白皮书》，说明了建造去中心化程序的目标并于2014年通过ICO众筹开始发展以太坊。以太坊致力于将区块链拓展应用于数字货币以外的领域，并为开发者提供一个能够快速创建智能合约以及去中心化应用的成熟开发平台。2015年12月，Linux基金会发起了Hyperledger[7]开源项目，Hyperledger旨在推动区块链的跨行业应用，提供了Fabric、Sawtooth、Burrow和Iroha等子项目。自2017年上半年以来，受新型募资方式ICO的影响，更多的资金和从业者加入区块链领域，极大促进了区块链技术的革新发展和区块链项目的不断落地。因此业内普遍认为2018年为区块链的“公链元年”，区块链技术进入了区块链3·0时代。

目前的区块链项目都是由不同团队基于不同的场景需求和设计理念，采用不同的技术架构开发出的异构区块链。由于区块链本身的技术特点，每个区块链都是一个孤立的P2P网络，因此这些项目就像是一个个相互隔绝的“信息孤岛”。如何实现区块链之间的互联互通和价值转移成为当前区块链技术的研究重点。如果说共识机制[8]是区块链的灵魂核心，那么跨链技术就是实现区块链之间互联互通和价值转移的关键[9]。跨链技术是区块链3·0时代的核心和关键技术。

1 跨链基础知识

1.1 跨链的产生

区块链技术和经济的发展，对区块链跨链提出明显的诉求。在性能上，区块链从基于PoW[10]的比特币和以太坊，发展到基于PBFT及DPoS共识算法的联盟链及公链网络，虽然实现了TPS（服务器每秒处理的事务数）从个位数到万级别的巨大提升，但是却以牺牲一定的“去中心化”为代价，这并不符合区块链的核心理念。区块链网络迫切需要在更好地保持去中心化理念的同时，大幅度提升区块链的交易性能。在功能上，伴随着智能合约[11]开发平台的逐渐丰富并完善，大量纷繁复杂的垂直公链及区块链商业应用显现，形成众多独立的基础设施和业务体系。这些区块链应用之间迫切需要实现功能上的扩展，即区块链间的互联互通，进而实现价值和业务的链间流转。在经济上，目前实现区块链网络之间价值转移的最常用方式是中心化的交易所，基于跨链技术搭建的去中心化交易所能够降低链间交易摩擦，提高价值流动性，成为中心化交易所的有效补充手段。

1.2 跨链的含义

跨链，顾名思义，就是通过某些技术让价值跨过链与链之间的障碍，使得原本存储在特定区块链上的价值转换为另一条链上的价值，从而实现价值的流通。跨链本质上和货币兑换是一样的。从业务角度讲，跨链技术相当于一个交易所，用户能够通过交易所进行跨链交易。跨链并没有改变每个区块链上的价值总额，只是不同持有人之间进行了价值的兑换。跨链不同于互联网的TCP/IP协议，传统的信息传输协议只需确保接收方收到完整准确的信息及发送方得到相应的反馈，如果传输过程中出现传输障碍，可以多次传输，不必考虑重复发送的问题。但账本之间的同步数据就需要确保两个账本的变动

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

是一致的，否则会出现双重支付或价值丢失的问题。在此过程中，信息传递只是两个账本同步数据的过程，而不是最终目的和结果。因此，跨链不只是信息的传输，其本质是在价值守恒的前提下，价值在不同区块链之间流动的过程。

1.3 跨链的类型

跨链的基础需求包括资产兑换和资产转移。资产兑换即将一条链上的资产（Token）兑换成等值的另一条链上的资产 ；资产转移则是将一条链上的资产转移到另一条链上，即将原链上的资产进行锁定，在另一条链上重新铸造等量等值的资产。资产兑换中每条链上的资产总量是不变的，只是资产所有权发生改变，且所有权的变更同时发生。资产转移是资产价值的转移，各条链上的资产总量随着转移的发生产生相应的增减。无论是资产兑换还是资产转移，重要的是保证跨链交易的原子性，即交易要么完全发生，要么完全失败，不存在第三种中间状态。目前对跨链的研究和应用落地主要集中在资产兑换和资产转移两个方面。有些项目提出了跨链智能合约的概念，通常指一条链上的智能合约能够确认原链跨链交易。由于需要对原链交易进行确认和验证，因此从基本原理和技术实现上来说，跨链智能合约和跨链资产转移非常相似。

1.4 跨链解决方案

从原理上讲，区块链跨链解决方案可分为嵌入式和非嵌入式。嵌入式解决方案需要把区块链互操作性逻辑集成到底层协议中，因此这种方案可以使时间和成本开销显著减少。但是这种方案显然存在隐患，即可能会在区块链网络中引入新的攻击载体或安全缺陷，这些缺陷可能会被不法行为利用。非嵌入式解决方案不需要定义区块链本身的互操作性逻辑。虽然这种方案可能需要权衡其便捷性，但比嵌入式解决方案要安全得多，而且不需要以任何方式修改现有的加密货币区块链。跨链的目的是建立资产价值和信息数据传输的通道，其逻辑架构一般包括连接方式、信息传输渠道、验证机制和信息反馈4个部分。一个完整的跨链解决方案要从项目愿景、适用场景和技术选型等方面统筹权衡，通过多种技术组合构成。

2 跨链技术难点及其参考解决方案

自 Blockstream[12] 公司提出侧链的概念以来，跨链一直是区块链技术的重点攻关方向。由于以往跨链需求程度并不高，技术上也存在着巨大难点，因此目前并没有普遍认可的跨链机制。当前跨链技术的难点及其参考解决方案主要集中在以下5个方面。

1）跨链交易验证问题

实现区块链之间的互联互通，首先要设计区块链系统之间的信任机制，使得一个区块链可以接收并验证另一个区块链上的交易。交易的确认和验证包含了两方面的问题，一是确认交易已经发生并且写入区块链账本，二是验证交易已经获得了系统中足够多区块的确认。目前常见的跨链交易验证机制有公证人机制和“ 区块头+SPV ”[13] 模式。公证人机制即通过外部公证人（联盟）验证跨链消息的可靠性，公证人验证通过后需对跨链消息签名。“ 区块头+SPV ”模式即将公证人（联盟）提供的外部区块链系统的区块头数据保存在自己的网络中，根据SPV机制验证交易。

2）跨链事务管理问题

一个完整的跨链交易可以拆分成若干个子交易，每个子交易在各自所属的区块链系统中进行处理。这些子交易构成一个事务，需要跨链事务管理，以保证事务的一致性和原子性[14]。跨链的事务管理又分为两个子问题，即交易的最终确定性问题和交易的原子性问题。在跨链事务管理中，为保证交易的最终确定性，通常有3种方案 ：等待足够多的确认数、区块纠缠和使用 DPoS[15]/xBFT 等共识算法。等待足够多的确认数是最简单粗暴的方法，其劣势就是事务处理的时间会变长。区块纠缠的原理是令两个链之间的区块存有依赖关系，当一个链上的某个区块被撤销时，自动撤销其他链上的相关区块。相比于 PoW 共识算法，DPoS 或 xBFT 等共识算法更容易达

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

成最终确定性，使用这类共识算法的区块链系统能更高效地实现跨链交易。交易的原子性是实现跨链交易的基本要求，也是跨链交易必须要解决的难点。

3）锁定资产管理问题

双向锚定是主链与侧链上的资产按照1:1兑换比例双向转移的过程。双向锚定设计方案中的关键问题是由谁来管理锁定账户并执行锁定和解锁等操作，如何保证锁定资产被安全地释放，而不会造成双花（Double-spending）[16]。另外，如何保证两条链的资产总量不变同样重要。关于锁定资产的管理，目前有单一托管人模式、联盟托管模式和智能合约模式。单一托管人模式是由一个单一托管人负责管理锁定的资产，执行并监管锁定资产的解锁操作。单一托管人模式虽然简单易行，但过于依赖中心化的托管人。较为去中心化的模式是联盟托管模式，当接到跨链的解锁请求时，联盟中的N个公证人都独立验证交易并投票，当投票数达到阈值M时，就能处置锁定的资产。智能合约模式则是为了更进一步地去中心化，该方案的前提条件是区块链系统能够支持智能合约，并且能够存储外部区块链的区块头来验证外部交易数据。

4）多链协议适配问题

随着区块链技术的发展和应用的不断落地，未来区块链生态系统必然是多链并存、互联互通的生态系统。多链互联互通蕴含着两层含义，一是已经存在的区块链系统如何实现互联互通；二是对于要开发的区块链，如何为其互联互通做好铺垫和准备。因此多链跨链方案可分为主动兼容型方案和被动兼容型方案。主动兼容型方案自上而下进行，主要针对已有的区块链系统，先有了上层不同的区块链应用系统，再进行底层的跨链机制研发。通常已有的区块链系统都是异构链，需要进行一一对接。被动兼容型方案自下而上进行设计，主要针对尚未开发的区块链系统，首先搭建好底层的跨链平台，然后基于跨链平台开发新的区块链系统，或者把现有的区块链系统简单、便捷、安全地接入平台，共享跨链平台的系统便利。

5）跨链安全保障问题

当两个系统发生交互时，难免会对彼此产生影响，若是链间安全无法隔离，那么如果一条链遭受攻击，将影响整个跨链网络。如何在跨链交易过程中保障自己系统和对方系统的安全性是值得思考的问题。总体来说，可以从以下3个方面考虑：适度隔离、检测安全事件和保障跨链交易正确性。链之间应该保持各自的独立性，尽量通过第三方节点或者独立模块处理跨链事务，这样当跨链交易发生问题时，不会影响链本身交易的处理。如果第三方节点或者独立模块具备检测安全事件的能力和响应能力，则在系统架构隔离的基础上更进一步，使跨链协议或系统具备类似防火墙的功能。

3 主流跨链技术

当前区块链之间在互联互通性上的欠缺极大限制了区块链的应用空间。区块链可以看作是孤立的数据库，没有用于数据输入或数据输出的适当接口。只有将同构或者异构的区块链网络连接起来，使资产和价值自由顺畅地在链间流通，才能实现真正的价值区块链网络。目前，主流的区块链跨链技术按照原理和实现方式可以分为4种：公证人机制（Notary Schemes）、侧链/中继（Sidechains/Relays）、哈希锁定（Hash-locking）[17]和分布式私钥控制（Distributed Private Key Control）。

3.1 公证人机制

当跨不同链的交易双方互不信任且信息不对称时，最简单的方法是寻找双方都信任的中介。公证人机制也称见证人机制，是通过选举一个或一组可信节点作为公证人，对区块链Y上是否发生了特定事件进行验证，并向区块链X上的节点进行证明。公证人群体通过特定的共识算法对事件是否发生达成共识。公证人模式是目前应用最广泛的一种模式，最大的单一公证人就是交易所。公证人机制是实现区块链之间互操作性的方案中较易实现的一种，无需进行复杂的工作量证明或权益证明，易于对接现有的区块链系统。

公证人机制分为中心化公证人机制（Centralized Notary Schemes）和多重签名公证人机制（Multi-sig Notary

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

Schemes)。中心化公证人机制运行处理效率相对较高，但是存在严重的单点故障风险，一旦公证人遭受攻击变得不可信，整个公证系统将停滞或处于较大的安全风险中。因此业界提出了多重签名公证人机制弱化中心化风险，该机制利用密码学技术，在每次交易验证时从公证人群体中随机选出一部分公证人，共同完成签名的签发，以降低对公证人可靠性的依赖程度。但该机制仍有潜在的作恶风险，仅作为目前的一种权衡方案。

采用公证人机制的典型项目有R3推出的Corda和Ripple实验室提出的The Interledger Protocol（ILP）[18]。

3.2 侧链 / 中继

侧链是相对于主链而言的一个概念，Blockstream对“侧链”的正式定义是“侧链是验证来自其他区块链数据的区块链”[19]。侧链协议本质上是一种特殊的跨链解决方案。这种解决方案可以实现从链*X*到链*Y*的价值转移和稍后从链*Y*回到链*X*的价值转移。通常将链*X*称为主链，将链*Y*称为侧链。当主链性能出现瓶颈或者某些功能无法扩展时，把资产转移到侧链上，相关交易就可以在侧链上执行，从而达到分担主链压力、扩展主链性能和功能的目的。

早期的侧链技术方案主要针对比特币提出。比特币的技术架构天生具有扩展性的不足，如交易延时长、吞吐量低以及不支持图灵完备的智能合约等，这些不足和缺陷必须通过重构比特币基础框架和算法才能解决。比特币作为市值最大、流通性最高、认可度最广的数字货币，修改其基础架构可能会引起巨大的风险，比特币核心开发者在技术升级的态度上也比较保守，这就决定了比特币很难通过技术升级提高自身的可扩展性。侧链技术就是另外启动一条区块链（侧链），将主链上的比特币资产转移到侧链上，反之也可以将侧链上的资产转回到主链上。比特币在主链和侧链上的资产双向转移称为资产的双向锚定（Two-way Peg）[19]。侧链上的资产有比特币的信用背书，价值上等同于主链上的比特币。同时侧链的设计架构不受主链的限制，开发者可以通过各种区块链技术构建侧链，应用于各种场景，所以侧链技术间接扩展了比特币的性能和功能。双向锚定是侧链实现的核心原理。双向锚定实施的安全性取决于区块链中的激励机制，以使参与双向锚定的关键方能够真正执行双向锚定所应实现的功能。双向锚定技术可通过以下模式实现：单一托管模式、联盟模式、SPV模式、驱动链模式和混合式设计[20]。

中继模式适用于链接两个异构或同构区块链，是实现区块链互操作性的更为直接的方式。该模式不完全依赖于可信第三方的验证判断，仅通过中间人收集两条链的数据状态进行自我验证，其验证方式依据自身结构不同而存在显著差异。

无论是侧链还是中继，最基本的需求就是采集原链信息。侧链与中继的区别在于：1）在从属关系上，侧链从属于主链，是主链与侧链之间去信任交互方案，且交易被限定在主链与侧链之间，更多地着眼于可拓展性而非可伸缩性；中继采用了中心辐射设计，不从属于某条主链，中继链更像是“调度中心”，只负责数据传递，不负责链维护。2）从执行过程看，侧链需要同步所有的区块头，验证区块链网络是否认可该项交易；中继不需要下载所有的区块头，因此拥有更优越的速度。3）在安全性方面，侧链的安全性建立在侧链能有效激励矿工进行交易一致性验证的基础上，主链的安全性无法在侧链上起作用；中继是由主链自行验证，安全性有一定保证。

侧链/中继的中继协议是从各主链抽象分离出一个跨链操作层，以避免受到主链的过多技术限制，保持中立的同时也能为自身项目积累价值。此外，中继链提供了统一的语言，可减少链路之间通信的安全隐患。总体而言，侧链/中继模式成本较高、效率较低，因为该模式下需要等待信息上链，确定不会发生回滚后才可确认。闪电网络（Lightning Network）、BTC Relay和RootStock等比特币侧链以及Lisk、Asch、Loom Network等非比特币侧链采用侧链技术实现跨链，Polkadot和

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

Cosmos[21] 等采用中继技术实现跨链。

3.3 哈希锁定

哈希锁定最早出现于比特币闪电网络的解决方案中，其通过资产锁定并设置相应的时间和解锁条件来实现公平交易。哈希锁定的基本流程为：链 X 上的账户 A 生成随机数 s，并发送 $hash(s)$ 给链 Y 上的账户 B；账户 A 在链 X 上锁定币，并设定条件，如果在时间 TA（当前时间+2x）内链 X 收到 s，则转账给账户 B，否则退回给账户 A；账户 B 收到 $hash(s)$，并看见账户 A 的锁定和时间设定后，在链 Y 上锁定币，并设定条件，如果在时间 TA–x 内链 Y 收到 s，则转账给账户 A，否则退回给账户 B；账户 A 看见账户 B 的锁定后，在时间 TA–x 内发送 s 给链 Y，得到链 Y 的币；账户 B 收到 s 后，在时间 TA 内发送 s 到链 X，得到链 X 的币。

哈希锁定是系统之间进行原子交易的基本框架，能保障跨链交易的原子性，可拓展应用于中心化账本或去中心化账本的系统之间。然而，哈希锁定只能实现跨链的资产兑换，即各链资产总量保持不变的情况下，资产的持有人变化，无法真正将资产转移至另一条链上。对于资产转移，还需要配合其他跨链技术方可实现。哈希锁定项目如闪电网络。

3.4 分布式私钥控制

分布式私钥控制通过分布式节点控制各种资产的私钥，并将原链资产映射至跨链中，确保各种资产在区块链系统中实现互联互通。分布式私钥控制的核心在于分布式控制权管理，即将资产的所有权和使用权分离，将原链上数字资产的控制权安全地转移至非中心化系统中。以区块链项目 Fusion[22] 为例，其实现通过数字资产的 Lock-in（锁定）和 Lock-out（解锁）两个基本步骤完成。在 Lock-in 过程中，将密钥分片并将分片密钥分布式保管，即分布式生成密钥；随后将资产转入原链上指定账户并由 Fusion 节点进行验证，实现控制权的分布式管理。Lock-out 过程也是如此，先检查 Fusion 映射账户中数据情况，满足具体条件后发起交易，Fusion 各节点通过各自保存的分片密钥进行验证，解除分布式控制权管理以及资产映射。分布式控制权完成交接后，智能合约将在 Fusion 映射账户中同步更新账户状态数据，以体现 Lock-in 和 Lock-out 完成情况，其记账过程实际上是通过 Fusion 系统向映射账户发放或收回等量等额数字资产的过程。

图 1 给出了 Fusion 项目中 Lock-in 过程示意图。

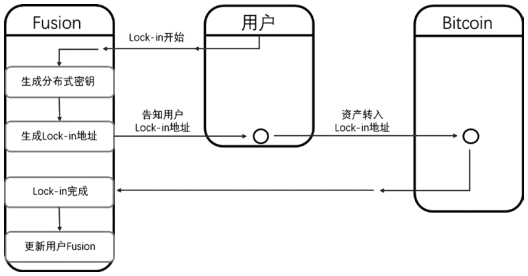

图 1 Fusion 项目中 Lock–in 过程示意图

分布式私钥控制类似于公证人机制，但用户始终拥有对资产的控制权，只是在存储数字资产的密钥上采用了分布式存储的方式，这在一定程度上避免了公证人机制下的中心化风险。此外，账户锁定不需要采用双向锚定方式，所有交易在验证节点重构后传入原链网络，不改变原链特性，各链均可自由且低门槛地接入原链，降低跨链接入成本，因此适用范围广，易于实现。但由于不改变原链特性，跨链需要根据原链的特性适配开发，因此开发难度较大，且等待原链确认时间较长，致使运行效率偏低。分布式私钥控制项目有 Wanchain、Fusion[23] 及 EKT 等。

3.5 跨链机制对比

表 1 给出了上述 4 种跨链机制的性能对比情况。

4 挑战与展望

区块链跨链沟通了众多价值孤岛，使得价值得以更广泛更顺畅地流动，因此跨链网络适用于底层平台扩容、支付结算、去中心化交易所、跨链钱包、主网资产映射、跨链预言机、资产抵押、实物链上资产交易、隐私保护[25]、医疗保健[26] 等诸多现实及潜在场景，其研究与建设对行业发展有着至关重要的作用。

4.1 挑战

虽然跨链技术能促进现有区块链生态显著发展，但

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

表 1 跨链机制性能对比分析

跨链机制 / 性能	公证人模式	侧链 / 中继	哈希锁定	分布式私钥控制
互操作性	所有	所有（需要所有链上都有中继，否则只支持单向）	只有交叉依赖	所有
信任模型	多数公证人诚实	链不会失效或受到 51% 攻击 [24]	链不会失效或受到 51% 攻击	链不会失效或受到 51% 攻击
使用跨链交换	支持	支持	支持	支持
使用跨链资产转移	支持（需要长期公证人信任）	支持	不支持	支持
适用跨链原语	支持	支持	不直接支持	支持
适用跨链资产抵押	支持（需要长期公证人信任）	支持	大多数支持但有难度	支持
多种币智能合约	困难	困难	不支持	支持
实现难度	中等	难	容易	中等

跨链技术目前仍处于初步探索阶段，尚未形成稳定体系，存在技术发展的不确定性，还有诸多问题有待解决。

1）跨链过程中两条链进行信息传输与交互，难免对原链系统产生影响。例如，权益冲击问题，尤其是基于 PoW[10] 共识的区块链系统，由于初期并没有多少矿工参与侧链挖矿，若此时主链的矿工算力远大于侧链，则主链侧链联通后会对侧链产生安全问题，造成权益冲击。因此，跨链技术不仅要充当连接者的角色，还需要具备适度隔离各链的功能。

2）目前区块链系统自身性能远未达到应用需求。例如，有的项目和方案通过双向锚定或哈希锁定的方式实现跨链，虽然能实现原子转账，但为保证资产安全转移，通常需要等待较长一段时间的确认期才能在其他链上解锁对应的数字货币，造成交易延迟。此外，交易延迟会随着网络拓扑结构的扩展进一步加剧。

3）商业落地应用较少。跨链项目主要集中于近两三年发起，跨链项目从数量上而言并不多，基于区块链底层基础设施开展的跨链项目多数仍处于概念验证阶段，实际应用尚未落地。跨链技术的尚不成熟、安全性及性能问题进一步限制了跨链项目的落地应用。

除上述之外，跨链网络之间的连接健壮性及安全性问题、跨链网络之间恶意行为的预警和制止问题、跨链交易中目的链的死循环问题、母链分叉问题、跨链网络激励制度的优化问题等，都是跨链技术的发展所面临的挑战。

4.2 展望

区块链从技术层面看是去中心化数据库和分布式账本，从商业层面看是价值网络。区块链要想获得大规模的商业应用，不仅需要实现平台间的信息互联，更需要实现区块链之间的信息互联。目前已有区块链系统支持保险、征信、资产证券化、知识产权和注册等商业场景，未来会有更多领域建立其自身区块链平台。跨链技术将带来不同场景的整合，塑造更具前景和活力的商业模式。

区块链跨链技术的发展将为云计算和物联网带来更多发展空间。区块链的技术特性可使数据更贴近计算节点，对传统云进行瘦身，为云计算装备新的引擎，促进新一代云计算架构的发展。区块链的技术特性契合物联网应用安全及发展的迫切需求[27]。基于跨链机制，使用与云计算融合的区块链，并通过网络中对数据的加密及共识解决物联网中数据和价值交换的安全性问题和可信性问题，必将加速推动人类社会迈入万物互联的新时代。

5 结束语

跨链技术是区块链 3.0 时代实现价值区块链网络的关键技术。本文对主流跨链技术进行了系统性的介绍和分析。现有跨链技术尚不成熟，研究角度不同、技术有别、应用场景各异，未来的区块链世界必然是多链共生的状态，因此仍需有持续攻关能力的科研团队和技术组织不断研究，不断探索实践。（责编 马珂）

参考文献：

[1] NAKAMOTO S. Bitcoin: A Peer-to-peer Electronic Cash System[EB/OL]. https://bitcoin.org/en/bitcoin-paper, 2019-4-9.

[2] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine Generals Problem [J]. ACM Trans on Programming Languages & Systems, 1982, 4(3): 382-401.

[3] WANG Xiliang, LIU Xuefeng, ZHAO Gansen, et al. Overview of Blockchain: Technology and Challenges[J]. Radio Communications Technology, 2018, 44(6): 531-537.

王锡亮，刘学枫，赵淦森，等 . 区块链综述 : 技术与挑战 [J]. 无线

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

电通信技术，2018，44（6）：531-537.
[4] SUN Yi，FAN Lingjun, HONG Xuehai. Technology Development and Application of Blockchain: Current Status and Challenges[J]. Engineering Science，2018, 20(2): 27-32.
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）：35-40.
[5] WOOD G. Ethereum: A Secure Decentralised Generalised Transaction Ledger[EB/OL]. https://gavwood.com/paper.pdf, 2019-4-11.
[6] BUTERIN V[EB/OL]. https://en.wikipedia.org/wiki/Vitalik_Buterin, 2019-4-13.
[7] Hyperledger[EB/OL]. https://www.hyperledger.org/, 2019-4-14.
[8] YANG Yuguang, ZHANG Shuxin. Review and Research for Consensus Mechanism of Block Chain[J]. Journal of Information Securyity Research, 2018(4): 369-379.
杨宇光，张树新 . 区块链共识机制综述 [J]. 信息安全研究，2018（4）：369-379.
[9] GAO Zhihao. Introduction to Cross-chain Technology of Blockchain[J]. Cards World, 2016(11): 46-51
高志豪 . 区块链之跨链技术介绍 [J]. 金卡工程，2016（11）：46-51.
[10] GERVAIS A , KARAME G O , WÜST K, et al. On the Security and Performance of Proof of Work Blockchains[C]// ACM. The 2016 ACM SIGSAC Conference, October 24–28, 2016 , Vienna, Austria. New York: ACM, 2016: 3-16.
[11] MA Chunguang, AN Jing, BI Wei, et al. Smart Contract in Blockchain[J]. Netinfo Security, 2018, 18(11): 8-17.
马春光，安婧，毕伟，等 . 区块链中的智能合约 [J]. 信息网络安全，2018，18（11）：8-17.
[12] Blockstream[EB/OL]. https://blockstream.com/, 2019-4-12.
[13] Mark Friedenbach, Compact SPV Proofs via Block Header Commitments[EB/OL]. http://sourceforge.net/p/bitcoin/mailman/message/32111357/, 2019-4-15.
[14] HERLIHY M. Atomic Cross-Chain Swaps[EB/OL]. https://arxiv.org/pdf/1801.09515.pdf, 2019-4-16.
[15] TAN Senpeng, YANG Chao. Research and Improvement of Blockchain DPoS Consensus Mechanism[J]. Modern Computer, 2019(6): 11-14.
谈森鹏，杨超 . 区块链 DPoS 共识机制的研究与改进 [J]. 现代计算机（专业版），2019（6）：11-14.
[16] KARAME G O, ANDROULAKI E, CAPKUN S. Double-spending Fast Payments in Bitcoin[C]//ACM. The 2012 ACM Conference on Computer & Communications Security, October 16–18, 2012, Raleigh, North Carolina, USA. New York: ACM, 2012: 906-917.
[17] ZHANG Shitong, QIN Bo, ZHENG Haibin. Research on Multi-party Cross-chain Protocol Based on Hash Locking[J]. Cyberspace Security, 2018, 9(11): 57-62, 67.
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）：57-62，67.
[18] HOPE-BAILIE A, THOMAS S. Interledger: Creating a Standard for Payments[C]//International World Wide Web Conferences Steering Committee. The 25th International Conference Companion on World Wide Web, April 11–15, 2016, Montréal, Québec, Canada. Republic and Canton of Geneva, Switzerland: International World Wide Web Conferences Steering Committee, 2016: 281-282.
[19] Vitalik Buterin. Chain Interoperability[EB/OL]. https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdfi, 2016-9-9/2019-4-7.
[20] BACK A, CORALLO M, DASHJR L, et al. Enabling Blockchain Innovations with Pegged Sidechains[EB/OL]. http://www.bubifans.com/ueditor/php/upload/file/20181015/1539599182599463.pdf, 2019-4-17.
[21] BUCHMAN E, KWON J. Cosmos: A Network of Distributed Ledgers[EB/OL]. https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md, 2019-4-17.
[22] Fusion[EB/OL]. https://www.fusion.org/,2019-4-15.
[23] PAN Chen, LIU Zhiqiang, LIU Zhen, et al. Research on Scalability of Blockchain Technology: Problems and Methods[J]. Journal of Computer Research and Development, 2018, 55(10): 2099-2110.
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.
[24] BAHACK L. Theoretical Bitcoin Attacks with less than Half of the Computational Power (draft)[EB/OL]. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.473.2485&rep=rep1&type=pdf，2019-4-18.
[25] WANG Hao, SONG Xiangfu, KE Junming, et al. Blockchain and Privacy Preserving Mechanisms in Cryptocurrency [J]. Netinfo Security, 2017, 17(7): 32-39.
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.
[26] GORDON W J, CATALINI C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability[EB/OL]. https://www.sciencedirect.com/science/article/pii/S200103701830028X, 2019-4-12.
[27]ZHAO Kuo, XING Yongheng. Security Survey of Internet of Things Driven by Block Chain Technology[J]. Netinfo Security, 2017, 17(5): 1-6.
赵阔，邢永恒 . 区块链技术驱动下的物联网安全研究综述 [J]. 信息网络安全，2017，17（5）：1-6.

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net