# 区块链跨链技术研究综述

沈传年
（国家计算机网络应急技术处理协调中心上海分中心，上海 201315）

**摘 要**：随着区块链技术的深入发展和持续创新，适用于不同应用场景和设计需求的区块链网络应运而生，区块链的相互独立性，不可避免地形成了区块链的价值“孤岛”效应。跨链技术是实现不同区块链之间业务协同和价值流通、提高其互操作性和可扩展性的重要技术手段。首先对跨链的基本概念进行了介绍，然后对跨链的技术难点、跨链主要机制的技术特点以及跨链的安全性问题进行了详细分析，最后引出了当前跨链技术所面临的挑战，并对未来跨链技术的发展进行了展望。

**关键词**：区块链；跨链；公证人；侧链；哈希锁定
**中图分类号**：TP309
**文献标志码**：A
**doi:** 10.11959/j.issn.2096−3750.2022.00301

# Review on cross-chain technology research of blockchains

SHEN Chuannian
Shanghai Branch of National Computer Network Emergency Response Technical Team/Coordination Center of China, Shanghai 201315, China

**Abstract:** With the in-depth development and continuous innovation of blockchain technology, blockchain networks suitable for different application scenarios and design requirements have emerged as the times require, the mutual independence of blockchains inevitably forms the value island effect of the blockchain. Cross-chain technology is an important technical means to realize industrial collaboration and value circulation between different blockchains and improve their interoperability and scalability. Firstly, the basic concept of cross-chain was introduced. And then, the technical difficulties of cross-chain, the technical characteristics of the main mechanism of cross-chain, and the security of cross-chain were analyzed in detail. Finally, the challenges faced by the current cross-chain technology were introduced, and the future development of cross-chain technology was prospected.

**Key words:** blockchain, cross-chain, notary, side chain, Hash-locking

## 0 引言

自 2008 年 Nakamoto[1]发表《比特币：一种点对点的电子现金系统》至今，比特币已历经 10 多年的发展，随着比特币规模和影响力的不断扩大，其底层核心支撑技术区块链[2-6]的研究和应用也正快速发展。区块链是一种分布式账本数据库，它通过块链式数据结构来验证与存储数据、通过分布式共识算法来生成和更新数据、通过密码学方法来保证数据的安全性，是涉及分布式账本、对等网络、智能合约[7]、共识机制[8]、加密算法等计算机技术的集成式创新应用，具有去中心化、去信任化、难以篡改和可追溯等特点，区块链正通过其颠覆性的创新技术构造着未来社会全新的信任体系和价值体系。

纵观区块链技术的发展阶段，2008–2013 年，以比特币为代表的区块链 1.0 的价值主要体现在数字货币[9]的应用上。2013 年，以以太坊[10]为代表的区块链 2.0 通过引入可编程化的智能合约为上层各类应用开发提供底层技术，开辟了区块链在数字货币领域以外的泛金融领域应用。随着区块链可扩展性的不断提高，自 2019 年下半年以来，区块链正

**收稿日期**：2022−04−28；**修回日期**：2022−09−19
**通信作者**：沈传年，scn3@qq.com

逐渐步入 3.0 时代。在 3.0 时代，区块链的应用范围将进一步拓展至政府、医疗、制造业等新领域，应用区块链技术改变现有业务运行模式正成为所有行业新的发展趋势。

然而，伴随区块链 3.0 时代的来临，单个区块链已远远不能满足社会各行业的技术需求，无法覆盖所有生产发展的应用场景，因此公有链[11]、联盟链[12]、私有链[13]等区块链项目应运而生。各类区块链是基于不同技术架构开发的，这就使得众多区块链彼此成为相互独立的价值体系，如何实现区块链之间安全高效的价值流通和业务协同已成为当前区块链技术研究的重点。跨链技术的出现，解决了单个区块链之间互联互通的需求，建立了平行区块链之间信息传输的渠道，提升了单个区块链的作用和数据使用价值，使得区块链真正意义上实现了去中心化的初衷。因此，跨链技术已成为区块链 3.0 时代的核心关键技术。

## 1 跨链技术概述

### 1.1 跨链的发展

在区块链技术发展的初期，信息的交互流通只限于在各个相互独立的单链之内，随着应用场景的日益丰富，单链的性能越来越难以满足实际应用需求，因此，基于单链分层技术（所有业务都建立在这条链的二层网络和侧链上）被广泛研究，并逐渐向多链、跨链阶段发展。

2012 年，Ripple 实验室提出了 Interledger 协议[14]，该协议是一种跨不同支付网络的安全、开放的跨账本支付协议，它允许任何在两个区块链账本上拥有账户的用户之间建立连接，以此实现全网信息的自由流通。

2013 年 5 月，TierNolan[15]在比特币论坛首次提出了原子交换方案，该方案概述了跨链加密货币互换的基本原则，其基本思想是当位于两个区块链上的交易用户在进行资产相互交换时，无须第三方参与，交易双方通过智能合约技术，并通过维护双方相互制约的触发器来确保资产交换的原子性。

2014 年 10 月，Blockstream 公司首次提出了楔入式侧链[16]技术，该技术使得比特币和其他账本资产能够在主链和其他区块链之间进行安全的转移。侧链技术的引入，不但可以解决主链运行效率低下的问题，而且侧链完全独立于主链，不会影响主链的安全性和稳定性。

2015 年 2 月，Poon[17]提出比特币闪电网络，闪电网络提出了两种类型的交易合约：序列到期可撤销合约（RSMC, revocable sequence maturity contract）和哈希时间锁定合约（HTLC, Hashed timelock contract），前者解决了链下交易确认的问题，后者解决了跨节点传递的支付通道问题。同年 12 月，Linux 基金会主导发起 Hyperledger[18]项目，该项目旨在推动区块链及分布式记账系统的跨行业发展与协作，为公开、透明、去中心化的企业级分布式账本提供开源标准。

2016 年，Blockstream 公司进一步提出了强联邦侧链[19]，强联邦侧链是一种可公开验证的、拜占庭式稳健的交易网络，可在无须第三方信任的前提下，促进任何交易在不同市场之间进行，通过引入联合区块签名机制减少交易延迟和改进互操作性。

2017 年，两大跨链头部项目 Cosmos[20]和 Polkadot[21]提出了搭建跨链基础平台方案，通过其平台支持兼容所有区块链应用[22]。

2018 年，多国区块链资深开发者共同发起国际跨链项目 Ether Universe（以太宇宙），Ether Universe 是世界首个基于 DPoS[23]机制的高性能的跨链项目，首创公证人机制+侧链混合技术实现高性能、低成本、低延迟的价值交换。

2019 年 7 月，中国区块链技术和产业发展论坛发布《区块链跨链实施指南》，提出了区块链的跨链实施框架，给出了跨链实施的应用构建、应用运行、应用评估和实施改进过程。

2020 年 12 月，中国信息通信研究院发布自主研发的跨链基础设施项目“可信链网”，旨在通过跨链技术，实现打通产业链上下游、横向业务联盟、链下数据通用服务和跨行业监管。

### 1.2 跨链的定义

跨链可以理解为是实现两个或多个独立区块链之间资产流通和价值转移操作的一种协议，当两个分布式账本中的用户进行价值转移时，跨链需要保证账本之间的数据同步，这就需要保证两个账本之间的操作变动一致，不然会导致账本之间出现双重支付及价值丢失等问题。跨链可实现不同区块链之间的价值转移，但是并不改变每条区块链上的价值总额。跨链技术的出现解决了区块链的可扩展性问题，实现了单个区块链的价值最大化，有效解决了长期以来单个区块链之间由于无法交互而产生

的价值“孤岛”问题。

### 1.3　跨链的类型

根据区块链底层架构的不同，跨链技术可以分为同构链跨链和异构链跨链两大类。传统意义上的跨链都是指同构链跨链，同构链跨链是指在具有相同底层架构的区块链之间实现价值的双向流通，同构链之间由于其共识算法、安全机制、区块生成验证逻辑都一致，因此，它们之间的跨链交互实现相对容易，目前虽有不少项目已使用了同构链跨链，但其却一直无法解决主流资产之间的交互实现；异构链跨链是指在不同结构的区块链之间实现跨链交互，异构链跨链类似区块链版的互联网底层协议，可以基于区块链所有的公链进行连接和交互，有望改变现有区块链应用局面，在异构链中，由于不同区块链的链式结构大相径庭，跨链交互时需要综合考虑不同区块链的结构差异，因此异构链的跨链交互实现难度比同构链要高很多，一般需要借助第三方服务辅助实现。

## 2　跨链技术难点

目前，跨链机制之所以未被业界普遍认可，一方面是由于当前中心化交易所尚可满足区块链基本交易需求，对跨链的需求还没到十分迫切的地步；另一方面是跨链技术还不够成熟完善，不同区块链之间的底层技术实现差异化较大，这给跨链技术的实现带来了重重障碍。跨链技术需要解决的难点问题主要集中在以下方面。

### 2.1　跨链交易原子性问题

通常情况下，一个完整的跨链交易由发生在不同区块链系统中的若干个子交易组成，这些子交易独立运行在不同的区块链系统中，交易的原子性[24]是指在交易处理过程中，如果交易处理的某个环节失败，前面的交易过程可以撤销，整个交易过程要么成功要么失败，不会存在部分交易环节成功，部分交易环节失败的情况。无法保证交易的原子性容易导致链间资产转移和兑换的过程中出现双重支付和资产凭空消失的问题。而在跨链技术中要保证交易原子性的难点就在于，跨链双方是彼此独立的不同的链，可能具有不同的共识算法、安全机制、数据结构以及交易处理逻辑等，这些都有可能造成交易最终没有被执行。因此，需要构建适用于通用场景的跨链交易原子性方案，提出相关的原子性保障理论。目前，可以通过哈希锁定实现跨链交易的原子性，哈希锁定通过使用时间锁和哈希锁[25]，让交易双方在锁定资产的前提下，在规定的时间内提供正确哈希值即可完成交易，否则交易失效，从而保证了交易的原子性。

### 2.2　跨链交易验证问题

跨链交易验证是指一个区块链可以对另一个区块链上的交易进行验证，验证包括两个方面：一方面是确认交易已经发生并且已被写入账本；另一方面是在跨链交易过程中，跨链的双方可以互相验证彼此的交易状态[26]。由于区块链系统需要保证链内信息的绝对可靠性，系统封闭性较强，一般无法主动获取链外信息，因此，原链上的交易信息相对于另一个区块链来说是一个外部信息，如何确保这个外部信息在进入另一个区块链时的正确性，是整个跨链机制的关键环节。如果通过分布式的方式验证原链上的交易状态，那么该问题的难度会更加复杂，即衍生为如何确保处理跨链的分布式节点不作恶，节点作恶的结果就是直接导致链间交易验证信息的错误，进而产生双花问题给跨链用户造成资产损失。目前，可以通过公证人机制[27]、“区块头+SPV”模式[28]实现跨链交易的验证，其中，公证人机制依靠受信任的第三方公证人来完成对链间交易信息的验证，而“区块头+SPV”模式通过保存外链系统的区块头信息，然后通过侧链机制中的 SPV 模式来对交易信息进行验证。

### 2.3　跨链交易资产管理问题

在跨链交易过程中，需要确保两个区块链的资产总量不会因为跨链交易而改变，进行跨链资产交易，必然会减少一个区块链上的资产，增加另一个区块链上的资产，这种交易过程使得每个区块链上的资产都相应发生了变化，而要保证这种资产变化的完全同步性，当资产跨出原链时，就必须要实现原链上资产的“锁定”状态，而当资产跨回原链时，原链资产被“解锁”，同时设定区块链上资产的“锁定”和“解锁”条件，可以有效管理跨链交易账户，确保“锁定”资产的隐私性和跨链交易的稳定性。因此，如何通过去信任的管理机制实现“锁定”和“解锁”功能，成为跨链交易能否成功的关键。目前，可以通过智能合约模式、侧链机制中的单一托管模式和联盟托管模式实现跨链交易资产管理[27]，其中，智能合约模式通过外链区块头信息验证外链交易数

据，单一托管模式通过受信任的托管人管理跨链资产的“锁定”和“解锁”，联盟托管模式则通过公证人联盟作为托管方来对跨链资产的交易进行管理。

## 3 跨链主要机制

当前，区块链底层技术平台呈现百花齐放、百家争鸣的态势，不同底层技术平台的区块链之间缺乏统一的互联互通机制，这极大限制了未来区块链技术和应用生态的发展空间。无论是对于公有链、联盟链还是私有链，无论是对于同构链还是异构链，跨链技术才是实现真正价值互联的关键所在。目前，相对成熟的跨链机制主要包括公证人机制、侧链/中继、哈希锁定、分布式私钥控制以及公证人+侧链混合机制。

### 3.1 公证人机制

公证人机制（notary scheme）是目前应用最广泛、技术实现最简单的一种跨链机制，在公证人机制中，假设区块链 A 和 B 本身是互不信任且不能直接进行互操作的，那么最简单的方法是引入一个双方共同信任的第三方作为中介，受信的第三方中介可以是一个中心化机构，也可以是一群节点，由这个共同信任的第三方中介进行跨链的数据收集、交易确认和验证。

公证人机制根据签名方式的不同，可以分为单签名公证人机制、多签名公证人机制以及分布式签名公证人机制。单签名公证人机制也叫中心化公证人机制，由单一指定的独立节点或者机构充当，承担了跨链数据收集、交易确认以及验证的任务，其优点在于交易处理速度较快、技术架构相对简单、兼容性好，但其中心化带来的安全性问题也较为明显。在多签名公证人机制中，公证人通常是由多个独立节点或者机构组成，每个节点都拥有自己的一个密钥，只有当达到一定比例的多个公证人在各自的账本上共同签名达成共识后，跨链交易才能被确认[1]，相较于前者，多签名公证人机制在部分节点受到攻击瘫痪时不至于影响整个系统的稳定性，通过减少对公证人的依赖，有效降低了中心化风险。分布式签名公证人机制采用多方计算（MPC, multi-party computation）的思想[29]，系统基于密码学仅生成唯一一个密钥，密钥被拆分成多个碎片，并将加密处理后的碎片分发给随机抽取的公证人，只有当允许的一定比例的公证人共同签名后，才能拼凑出完整的密钥，从而完成更加去中心化的跨链交易过程，相较于前两者，安全性更高，但其技术实现也更为复杂。

公证人机制的代表项目主要有 Interledger、Palletone 等。Interledger[14]协议在进行跨链交易确认时引入一个或一组诚实可靠的第三方节点作为公证人，由公证人充当两个不同区块链记账系统的“连接器”，当参与方均对交易内容达成共识时，便可进行链间资产转移，该协议提供两种支付模式：在原子模式下，转账由参与者选择的一组特别公证人协调，以确保所有转账要么执行要么中止，在通用模式下，则使用激励措施来满足对任何相互信任的系统或机构的需求。Palletone[30]协议通过使用独有的“陪审团+调停中介”双重共识机制实现跨链资产交互，因其结合使用了陪审团共识算法和有向无环图（DAG，directed acyclic graph）[31]数据存储，使得智能合约执行和数据存储可以并行处理，在计算性能和数据存储方面均突破了传统区块链的技术限制。

针对公证人机制的跨链研究，戴炳荣等[32]针对公证人机制中节点信用监督不足问题，提出了一种基于改进 PageRank 算法的跨链公证人节点信用评价模型，该模型通过改进的 PageRank 算法对公证人节点的信用进行计算，去除信用度低的公证人节点，从而保证跨链交互的安全性。蒋楚钰等[33]针对公证人机制中公证人的节点职能过于集中以及跨链交易处理效率低等问题，提出了一种基于公证人组的跨链交互安全模型，该模型将公证人节点按照职能分为交易验证者、交易连接者和交易监督者，3 类节点各司其职，协同完成跨链交易。其安全性分析表明，该模型在保证信息机密性和完整性的同时，极大地提高了跨链交互效率。

### 3.2 侧链/中继

侧链（side chain）是一个独立于主链的区块链系统，通过设计按需定制的协议、账本、共识机制、智能合约等，使用户可以在侧链上使用主链的代币进行跨链交易，跨链交易中侧链与主链沟通的过程被称为双向锚定（two-way peg）[34]，具体而言就是，在主链上锁定交易后，等量等值的代币才能在侧链上被释放，而当等量等值的代币在侧链上被锁定时，主链上的原始币就可以被释放了，因此，双向锚定就是主侧链双方判断一方是否解锁，要以另一方是否已经有投币行为为准。当前，双向锚定技术

的实现方式主要包括以下 4 种模式。

1) 托管模式

托管模式的基本原理与公证人机制类似，根据受信的第三方机构不同，可以分为单一托管模式和联盟托管模式。单一托管模式由交易参与方将数字资产发送到一个主链单一托管方，当单一托管方收到相关信息后，就在侧链上将相应数字资产发送给交易方侧链账户；联盟托管模式使用公证人联盟作为资产托管方，利用公证人联盟的多重签名对侧链的数字资产流动性进行确认，以缓解单一托管模式过度中心化的风险。

2) SPV 模式

简单支付验证（SPV, simplified payment verification）是一种特定的工作量证明机制，通过少量数据就可以验证一个支付交易是否已经在区块链中发生[35]。交易用户在主链上将数字资产发送到主链的一个特殊地址，以锁定主链的数字资产，然后创建一个 SPV 证明并发送到侧链上，这时，一个对应的带有 SPV 证明的交易会出现在侧链上，同时验证主链上的数字资产是否已经被锁住，然后就可以在侧链上打开具有相同价值的另一种数字资产，当数字资产返回主链时，过程与之相反。SPV 模式是去中心化双向锚定技术的最初设想，其存在的问题是需要对主链进行软分叉[36]。

3) 驱动链模式

在驱动链中，矿工作为算法代理监护人，对侧链当前的状态进行检测，监管被锁定的数字资产，矿工们通过投票决定何时解锁数字资产以及将解锁的数字资产发往何处。当诚实矿工在驱动链中的参与程度越高，系统安全性也就越大，与 SPV 模式一样，驱动链模式也需要对主链进行软分叉。

4) 混合模式

以上双向锚定模式在主链和侧链上是对称的，如果主链使用 SPV 模式，侧链也使用 SPV 模式，混合模式则是将以上双向锚定模式进行有效结合的模式，在主链和侧链上使用不同的解锁方法，例如在主链上使用 SPV 模式，而在侧链上使用驱动链模式。同样，混合模式也需要对主链进行软分叉。

5) 4 种模式比较

双向锚定技术优缺点见表 1，从对 4 种模式的比较来看：在实现方式方面，托管模式无须对现有比特币协议进行任何改变，而其他 3 种模式则需要在兼容现有主链的情况下对协议进行改造；在模式结构方面，托管模式、SPV 模式和驱动链模式都是对称结构，即主侧链均使用相同的模式，混合模式则使用不同的模式；在安全性方面，托管模式因需要借助第三方，存在中心化风险，虽然联盟托管模式一定程度上缓解了单一托管模式过度中心化的风险，但安全性仍较低，SPV 模式通过链上节点验证，避免了中心化风险，而驱动链模式的安全性完全取决于诚实矿工的参与数量，混合模式的安全性则取决于所使用的模式。

中继（relays）是对公证人机制和侧链机制的有效融合和延伸，中继链旨在构造一个第三方公有链，通过跨链消息传递协议，连接区块链网络中的其他链，通过在主链和侧链之间加入一个通道，通道内创建一种特定的协议，使得参与交易的所有区块链都可以通过该通道内的特定协议进行跨链数据交互，这个加入的通道就称为中继链。

**表 1　　双向锚定技术优缺点**

| 模式 | 优点 | 缺点 |
|---|---|---|
| 托管模式 | 托管模式不需要对现有协议进行任何改造；<br>联盟托管模式中公证人联盟的诚实度越高，系统的安全性越高 | 单一托管模式存在过度中心化风险；<br>联盟托管模式中公证人联盟仍存在共谋风险 |
| SPV 模式 | SPV 模式在进行交易验证时，由于只验证区块头信息，无须验证所有交易记录，可提高交易处理速度；<br>通过将小额零散交易转移到侧链进行，一方面可以缓解主链的交易负担，提高交易效率，另一方面可以有效保护主链上大额资产账户的地址；<br>可扩展主链的功能，提供更多的跨链应用场景 | 需要在兼容现有主链的情况下对协议进行改造；<br>SPV 模式由于只保存了区块头信息，无法验证全部交易记录，存在被恶意攻击的安全风险；<br>需要对主链进行软分叉 |
| 驱动链模式 | 诚实矿工的参与数量越多，系统的安全性越高 | 需要在兼容现有主链的情况下对协议进行改造；<br>需要对主链进行软分叉 |
| 混合模式 | 主链和侧链使用不同的模式，通过整合多种模式的优点，弥补了单一模式的不足 | 需要在兼容现有主链的情况下对协议进行改造；<br>需要对主链进行软分叉 |

侧链和中继的相同点在于在跨链交易过程中都需要采集原链信息，而不同之处在于：在从属关系上，侧链从属于主链，而中继没有从属关系，负责跨链数据的传输；在执行过程方面，侧链由于需要同步所有的区块头以验证交易是否被认可，因此在效率方面不及中继[37]；在安全性方面，由于侧链和主链的安全机制是独立的，故主链的安全优势无法在侧链上体现出来，而中继则是由主链自行验证，因此安全性更胜一筹[38]。

侧链/中继机制的代表项目主要有 BTC Relay、Cosmos 等。BTC Relay[39]通过使用以太坊的智能合约实现以太坊网络和比特币网络的去中心化连接，使用户可以在以太坊上对比特币进行交易验证，BTC-Relay 利用 BTC 区块头在以太坊上创建一个小型简要版的比特币区块链，解决了在以太坊中进行 BTC 支付的问题。Cosmos[20]基于 Tendermint[40]共识机制采用中继链的方式实现跨链交互，Cosmos 网络结构包括 Hub、Zone、IBC 3 个组成部分，其中 Zone 是 Cosmos 中的不同区域空间，类似接入的不同区块链，而 Hub 是 Cosmos 的中心网络，负责追踪记录每个 Zone 的状态，Hub 与 Zone 之间通过跨链通信（IBC, inter-blockchain communication）协议进行消息传输。

针对侧链/中继机制的跨链研究，云闯[41]针对区块链发展中存在的可扩展性问题，提出了一种一主链多侧链系统架构的设计方案，该方案通过动态索引连接主侧链，基于 Merkle[9]路径进行跨链交互，交易处理方面，通过将侧链交易进行分组，并将分组后的交易交由 Worker 集群进行处理，以实现侧链交易的并发处理。实验表明该方案能显著提高系统交易处理能力，系统交易吞吐量可随着侧链数量的增加而保持稳定。刘晶等[42]针对传统区块链访问控制策略效率低、安全性差等问题，提出了一种基于主侧链合作的工业物联网访问控制策略，该策略使用 Plasma 方案[43]对区块链的侧链进行扩容，侧链负责智能合约的执行，并与主链进行批量数据验证，以实现主侧链之间数据的高效交互，在访问控制模型的设计上，实现访问控制的数据存储与策略执行相分离，以增强数据的安全防护。实验表明，该策略能够提高基于工业物联网区块链控制策略的管理效率以及安全性。

### 3.3 哈希锁定

哈希锁定（Hash-locking），全称哈希时间锁定合约（Hash timelock contract），最早于 2013 年在 bitcointalk 上被提出，后被成功应用于比特币的闪电网络中，哈希锁定巧妙地使用时间锁和哈希锁[25]，让交易双方先锁定资产，如果都在规定的时间内输入正确哈希值的原值，即可完成交易，否则交易失效，从而保证了交易的原子性。其中，时间锁是指交易双方约定在某个有限的时间内输入正确哈希值的原值才有效，超时则承诺失效；哈希锁是指对一个哈希值 $H$，如果提供原像 $R$ 使得 Hash($R$)=$H$，则承诺有效，否则失效。

哈希锁定的基本原理是：链 A 上的账户 $A_X$ 生成随机数 $r$，并发送 Hash($r$)给链 B 上的账户 $B_Y$，同时账户 $A_X$在链 A 上将数字货币锁定在智能合约中，并设定交易的时间限制，账户 $B_Y$收到 Hash($r$)，看到账户 $A_X$的锁定和时间设定后，在链 B 上使用 Hash($r$)将数字货币锁定在智能合约中，并设定交易时间限制，账户 $A_X$看到账户 $B_Y$的锁定后，在规定时间内，发送包含随机数 $r$ 的认领协议给账户 $B_Y$，账户 $B_Y$收到认领协议后在规定时间内给出哈希值，锁定的数字货币立即释放，完成交易。否则跨链交易失败，交易参与方拿回各自在智能合约中的资产。

哈希锁定的优点是交易参与方无须彼此信任，资产锁定实现了质押效果，无须将资产托管给第三方公证人，安全性相对较高，同时由于设定了交易时间限制，交易发起者不用浪费时间持续等待，可以有效避免恶意拖延交易的行为，降低了交易的风险；缺点是哈希锁定只能实现跨链资产的交换，而不能实现跨链资产的转移。

哈希锁定机制的代表项目主要有闪电网络。闪电网络[17]是一个双向支付渠道网络，它将两个节点在比特币区块链的链下即第二层进行交易处理和账本变更，然后在链上即第一层进行结算确认，从而避免大量实际交易资金的转移，一定程度上提高了交易效率并降低了交易费用。

针对哈希锁定机制的跨链研究，张诗童等[44]提出了一种基于哈希锁定的多方跨链协议，该协议使用 $N$ 方协议“边着色”自动撮合算法，在多链情况下为 $N$ 个人 $M$ 种货币交易进行快速匹配，且保证了交易的原子性和公平性，该算法无须第三方交易所，解决了现有交易所中心化导致的信任问题。李祖建[45]针对哈希锁定机制现实应用场景中违约成本低、交易周期长等问题，提出了一

种改进算法，该算法通过引入交易回撤机制、履约保证金、增加抗攻击性，有效提高了跨链交易性能，增加了攻击者的攻击成本，降低了跨链交易风险。刘峰等[46]提出了一种基于改进哈希锁定跨链资产交互协议，该协议在 Fabric 区块链引入了中间人账户概念，使得 Fabric 和以太坊之间可以进行对等资产交互，有效扩展了 Fabric 与其他区块链的跨链方式，仿真结果表明，该协议具备可行性，并且实现了跨链交易的高效性和安全性。

### 3.4　分布式私钥控制

分布式私钥控制（distributed private key control）基于分布式密钥生成技术[47]和门限密钥共享技术[48-49]，将链上数字资产的所有权和使用权分开管理，通过引入锁定和解锁两种操作，对各数字资产私钥进行分布式控制管理，并将原链数字资产映射到新的中间链上，实现了对原链数字资产控制权的去中心化管理，通过新的中间链进行跨链资产交换和价值转移。在跨链过程中，资产的锁定和解锁由所有参与节点共同决定，任何未达门限值的单个节点或少数联合节点都无法拥有资产的使用权。

分布式私钥控制机制的代表项目有 Wanchain 和 Fusion。Wanchain[50]要求不同区块链首次接入时，需要在它的平台上完成注册，以确保对不同区块链资产的唯一识别，Wanchain 的创新之处在于一是实现了完全去中心化的跨链资产账户管理功能；二是通过增加验证节点，并进行节点间共识，大大降低了其他链的接入门槛；三是通过门限密钥共享和环签名等技术方案确保了交易隐私。在 Fusion[51]项目中，以其与比特币的交互为例，在锁定阶段，节点 A 向 Fusion 发起资产锁定请求，并通过智能合约将密钥随机分发给不同节点，A 在收到智能合约返回的公钥地址后将资产锁定，智能合约在确认 A 资产锁定后更新其在 Fusion 中的资产；在解锁阶段，节点 A 向 Fusion 发起资产解锁请求，智能合约确认 Fusion 中 A 的资产后，广播解锁交易签名请求，对应的私钥节点检查解锁交易后签名，并在平台进行广播，将锁定的资产转移到 A，智能合约确认解锁后更新 Fusion 中 A 的资产。

### 3.5　公证人+侧链混合机制

公证人+侧链混合机制（notary scheme + sidechains mixing technology）[22]结合了公证人机制操作实现简单、无须复杂工作量证明以及侧链低成本、快速高效的优点，通过区块链之间彼此信任的分布式节点作为公证人实现跨链资产的快速交互，避免了中心化问题，同时，通过侧链技术实现链间高效的通信交互。

公证人+侧链混合机制的代表项目有 Ether Universe 和 Sifchain。Ether Universe 是第一个采用公证人+侧链混合机制基于 EOSIO 3.0 平台技术的跨链服务方案，使用分布式节点进行连接，首创公证人、担保人、矿工的混合 DPoS[52]共识机制，在交易性能、降低成本、稳定性、安全性等方面均实现了重大提升。Sifchain 基于 Cosmos[20]区块网络和 Tendermint[40]共识算法构建，使用双向锚定和 IBC 协议，实现包括比特币、以太坊、币安链等在内的 20 多条主流区块链的跨链集成，具有高性能、低成本、高扩展性等优点。

### 3.6　5 种跨链机制比较

为了更全面直观地展现上述 5 种跨链机制各方面的差异，本文从互操作性、信任模型、是否可用于跨链交换、是否可用于跨链资产转移、是否可用于跨链预言机、是否可用于跨链资产抵押、跨链实现难度、跨链交易效率、跨链安全性以及代表项目等多个维度对 5 种机制的性能进行简要比较，跨链主要机制性能对比见表 2。

在互操作性方面，哈希锁定因在交易过程中资产的锁定和解锁需要触发区块链双方，存在交叉依赖的关系，因此相对其他机制有着明显的不足；在信任模型方面，公证人机制因需要可信任的第三方作为公证人，存在中心化风险，其他机制则不会涉及此问题；在跨链交换方面，5 种机制均支持跨链资产交换；在跨链资产转移方面，由于哈希锁定的原子交换保证了同一条链上的资产总量不变，因此，哈希锁定只能用于跨链资产的交换，而无法实现跨链资产的转移，而其他机制均可实现资产转移功能；在跨链预言机方面，5 种机制中只有哈希锁定不直接支持跨链预言机[9]操作；在跨链资产抵押方面，5 种机制均支持跨链资产抵押，其中，哈希锁定在大部分场景下支持跨链资产抵押；在跨链实现难度方面，公证人机制中的单签名公证人机制技术架构相对简单，而分布式签名公证人机制技术实现较为复杂，综合来看其实现难度中等，侧链中除托管模式外，其他 3 种模式均需要在兼容现有主链的情况下对协议进行改造，实现复杂度较高，同理，公证人+侧链混合机制实现难度也较高，哈希锁定通过智能合约实

表 2　　跨链主要机制性能对比

| 跨链机制性能 | 公证人机制 | 侧链/中继 | 哈希锁定 | 分布式私钥控制 | 公证人+侧链混合机制 |
|---|---|---|---|---|---|
| 互操作性 | 所有 | 所有（所有链都须支持中继，否则只支持单向操作[27]） | 只支持交叉依赖 | 所有 | 所有 |
| 信任模型 | 多数公证人诚实 | 所有链不会失效 | 所有链不会失效 | 所有链不会失效 | 混合模式 |
| 是否可用于跨链交换 | 是 | 是 | 是 | 是 | 是 |
| 是否可用于跨链资产转移 | 是（需要公证人一直受信任） | 是 | 否 | 是 | 是 |
| 是否可用于跨链预言机 | 是 | 是 | 不能直接使用 | 是 | 是 |
| 是否可用于跨链资产抵押 | 是（需要公证人一直受信任） | 是 | 大多数支持 | 是 | 是 |
| 跨链实现难度 | 中 | 高 | 低 | 中 | 高 |
| 跨链交易效率 | 低 | 低 | 中 | 中 | 高 |
| 跨链安全性 | 低 | 低 | 中 | 中 | 高 |
| 代表项目 | Interledger<br>Palletone | BTC Relay<br>Cosmos | 闪电网络 | Wanchain<br>Fusion | Ether Universe<br>Sifchain |

现跨链交互，是一种较易实现的跨链机制，分布式私钥控制不需要改变原链特性，但智能合约需要根据原链特性适配开发，有一定的实现难度；在跨链交易效率方面，公证人机制中公证人在有限时间内只能实现单笔跨链交易的验证审核，无法对多笔交易进行批量处理[33]，这在一定程度上降低了交易的效率，侧链需要等待信息上链，明确不会发生回滚才能确认，交易效率较低，哈希锁定在跨链交易过程中链与链之间无须相互了解，一定程度上促进了交易效率，分布式私钥控制因跨链交易等待原链的确认时间较长，因此交易效率中等，公证人+侧链混合机制借助分布式节点公证人实现了跨链交易的快速交互，具有较高的效率；在跨链安全性方面，公证人机制存在中心化风险，侧链由于主侧链安全机制相互独立，主链安全优势无法在侧链上体现，因此这两者安全性都较低，哈希锁定因无须依赖第三方，具有去中心化的特点，安全性较好，分布式私钥控制实现了对原链资产控制权的去中心化管理，资产的锁定和解锁由节点共同决定，安全性也较好，而公证人+侧链混合机制由于使用分布式节点作公证人，有效避免了中心化的风险，具有较高的安全性。

根据上述 5 种跨链机制的比较可以得出结论：每一种跨链机制根据自身的技术实现方式都存在其优缺点，目前为止还没有出现一种能满足所有应用场景需求的全能的跨链机制，当下，跨链机制的使用，应结合具体应用场景和跨链机制本身的特点进行选择。

## 4　跨链安全性分析

跨链技术及应用出现的时间并不长，目前还处于刚刚兴起的阶段，由于其在跨链速度、交易性能、资产管理等方面都还存在很大的提升空间，因此现有跨链技术尚未获得广泛应用。然而跨链技术所面临的最大需求似乎还不是上述问题，而是迫在眉睫、亟待解决的安全性问题，近年来，一系列跨链应用领域的安全事件频频发生，金额巨大，跨链安全性问题已成为制约跨链技术发展的重要因素。本文将分别从跨链机制、攻击类型两方面对跨链的安全性问题进行简要分析。

### 4.1　不同跨链机制安全性问题

根据上述跨链机制的比较可知，在跨链安全性方面，除公证人+侧链混合机制的安全性相对较高外，其他几种跨链机制因其在技术原理与设计实现等方面存在的缺陷，均在不同方面存在着一定的安全性问题，本文重点对目前常用的公证人机制、侧链/中继、哈希锁定 3 种跨链机制的安全性问题进行简要分析。

#### 4.1.1　公证人机制安全性问题

公证人机制是一种技术实现相对简单的跨链机制，能够支持不同结构的底层区块链[53]。但公证人机制本质上是一种中介方式，由于其引入了第三方机构，中心化程度较高，跨链价值转移完全掌控于第三方公证人的诚实性，只有第三方公证人完全真实可信，才能确保跨链交互的安全性[54]，因此中心化风险较高，虽然可以通过多签名公证人机制以

及分布式签名公证人机制在一定程度上提高其安全性，但并不能完全实现去中心化，其共谋风险依然存在[55]。

#### 4.1.2　侧链/中继安全性问题

侧链是一个相对独立于主链运行的区块链，因此，侧链和主链的安全机制也是独立的，侧链在跨链交易过程中需要同步所有的区块头以验证交易是否被认可，无法获取主链网络上所有的交易信息，因此，也就无法对主链交易信息进行全面验证和追溯[53]，也无法对常见区块链的攻击进行识别[55]，故主链的安全优势无法在侧链上体现出来。而中继本质上是对公证人机制和侧链机制的有效融合和延伸，是一种去中心化的公证人机制，虽然较侧链的安全性有所提高，但其与各平行链的安全性在一定程度上也会受到链双方的影响[54]。

#### 4.1.3　哈希锁定安全性问题

根据哈希锁定的工作机制，参与交易的各方无须彼此信任，通过资产锁定实现质押，因此，无须将资产托管给第三方，相对于公证人机制，其安全性较高，而且由于设定时间锁定，有效避免了恶意拖延交易的行为，有效降低了交易风险，但是哈希锁定在一定程度上也受时间锁定和资金锁定机制影响，其安全性问题主要表现为：因哈希锁定有时间锁定限制交易时间，如果有恶意交易方在短时间内建立大量资产交易，并故意让所有交易同时超时，将会在网络中造成大量超时交易的无用信息，从而阻塞正常交易信息的发送；哈希锁定的资产锁定阶段，交易双方必须以“热钱包”[56]方式保持一直在线连接区块链网络的状态，以便交易双方能及时对交易反馈结果进行签名验证，这也增加了黑客攻击“热钱包”，盗取交易用户私钥，从而窃取用户钱包资产的风险[57]。

### 4.2　不同攻击类型安全性问题

在跨链网络中，作为区块链重要组成的共识机制因其决定了链上节点以何种方式对数据达成一致，故在很大程度上决定了区块链系统的安全性，因此，基于工作量证明、权益证明等的共识机制是攻击者实施攻击的主要方向，攻击者会根据不同的共识机制，采用不同的攻击方式来破坏区块链系统的正常运行，以获得额外收益。此外，针对共识机制以外的其他方面的攻击也正成为威胁跨链安全的重要方面[58]。本节将对双花攻击、日蚀攻击、女巫攻击、竞争条件攻击、长程攻击以及重放攻击 6 种攻击方式所带来的跨链安全性问题进行简要分析。

#### 4.2.1　双花攻击

双花攻击（double spending attack）也叫双重支付攻击，简单来说就是同一笔钱被花了两次，是指攻击者通过不间断发起和撤销交易，将同一笔数字资产反复使用以实现获利的行为。目前双花攻击包括 51%攻击、芬妮攻击、种族攻击、Vector76 攻击以及替代历史攻击 5 种攻击方式[59]，以 51%攻击为例，攻击者把一定数量的代币投放到交易所，等交易被确认后，将所投放代币进行兑换，当攻击者拥有超过 51%算力时，通过分叉[60]直接创建一条新链进行挖矿，根据最长链原则[61]，当新链长度超过原链时，原链被舍弃，新链成为主链，原链投放的代币重新回到攻击者手中，而此时攻击者已经获得了之前交易的兑换金，最后攻击者可以在新链上继续使用这些代币，实现双花。Rosenfeld[62]推导出了成功双花的概率，给出了各种形式，并讨论了双花的经济可行性条件，最后证明了通过 6 次等待就能获得绝对安全以及将等待时间长度作为确定安全的主要因素是不成立的。双花攻击一般发生在一致性较弱的区块链系统[23]，在跨链交易过程中，一个完整的跨链交易通常包括多个子交易，这些子交易一般独立分布在不同区块链系统中，跨链系统必须确保交易的原子性，即交易必须同时成功或者同时失败，在成功执行一次跨链交易后，其子交易也能成功执行，如果任一子交易执行失败，要能撤回前面已完成的子交易。如果无法保证跨链交易双方交易信息的一致性和同步更新[22]，则跨链过程中不可避免会出现双花攻击问题[63]。

#### 4.2.2　日蚀攻击

日蚀攻击（eclipse attack）是一种基于对等网络（P2P, peer-to-peer）的攻击方式，由于 TCP 连接限制，在比特币网络中，单个节点连接其他节点的数量有限（对内连接为 117 个节点，对外连接为 8 个节点），攻击者如果对受害节点的连接目标节点发起攻击，并接管所有连接目标节点，那么攻击者将会完全控制受害节点的所有输入和输出信息，无法获取真实的网络信息，攻击者相当于在受害节点和区块链网络中建立了一个第三方中间人，受害节点只能接受攻击者希望它收到的信息，此时称受害节点被攻击者“日蚀”。延伸来看，攻击者可结合“日蚀”攻击来进行双花攻击[23]，即攻击者可以通过控制交易节点的输入信息，致使交易节点信息缺失，

让交易节点和自己的交易在其生成的私链上进行，而实际区块链上并不存在该交易，以成功实施双花。Heilman 等[64]提出了对比特币对等网络的“日蚀”攻击，该攻击允许攻击者控制足够数量的 IP 地址来垄断与受害比特币节点之间的所有连接，以破坏比特币的核心安全保障。Marcus 等[65]提出了对以太坊节点的“日蚀”攻击，该攻击使用两台均只有一个 IP 地址的主机进行攻击，并认为被攻击漏洞是由于以太坊采用 Kademlia 点对点协议造成的，最后提出了抵御对策，该策略提高了“日蚀”攻击的门槛。相较于比特币、以太坊等这类全球节点分布广泛且数量巨大的大型公有链网络都易遭受“日蚀”攻击，跨链网络中的交易节点相对更少也更集中，因此在跨链交易过程中更容易遭受“日蚀”攻击[55]。

#### 4.2.3 女巫攻击

女巫攻击（sybil attack）[66]在跨链中存在的背景是基于区块链的数据冗余机制[67]，即同一节点的数据一般需要备份到多个不同分布式节点，它是攻击数据冗余机制的一种非常有效的方式。女巫攻击是指一个恶意节点通过在区块链网络中创建多个伪装身份的节点[68]，并将这些伪装节点在整个区块链网络上进行广播，当其他正常节点需要通过这些伪装节点查询信息时，恶意节点可以操控伪装节点返回虚假信息或者拒绝返回信息，当区块链中的伪装节点数量大于真实节点数量时，攻击者会凭借领先的投票优势来击退真实节点，并拒绝接收新的节点加入网络，以达到对整个区块链网络的控制，进而实施更改交易顺序或记录，甚至逆转交易等恶意行为。公有链因其共识机制不依赖于节点数量，基本不存在女巫攻击的风险，而联盟链为了提高其共识效率，将节点数量控制在了一定的范围内，这就使得女巫攻击有了可乘之机。在跨链交易过程中，当跨链交易方为联盟链时，同样也会面临女巫攻击的风险。2022 年 4 月，跨链协议 Hop Protocol 表示为了对抗女巫攻击，将计划向识别和举报女巫地址的社区成员奖励 25%的代币，女巫攻击者也可以通过自我举报来获得奖励，该政策自发布以来，已收到大量举报。

#### 4.2.4 竞争条件攻击

竞争条件攻击（race condition attack）是指，在跨链交易过程中，尤其是原子交换类的跨链系统[55]在跨链交易确认时，都会存在交易确认的先后顺序，理论上来讲，任何参与跨链交易的一方，无论是发起方还是接收方，都有可能被最先确认交易，这就可能导致出现竞争条件攻击问题[22]。比如说，跨链交易双方 A 和 B 通过智能合约进行 BTC 和以太币（ETH, Ethereum）资产交易，发起方 A 将一定数量的 BTC 发送至合约指定的地址，接收方 B 将等值的 ETH 也发送到合约指定的地址，此时可能存在这种情况，即接收方 B 也可以向合约指定的相同地址发送与 A 相同数量的 BTC，如果 B 的交易被最先确认，那么 B 就能在得到 A 的 BTC 的同时，还能拿走之前自己转入合约地址中的 ETH，而发送方 A 不但无法获取 B 的 ETH，还会损失了自己已转入的 BTC。竞争条件攻击一般是针对用户账户余额这个条件进行的竞争，只要用户账户始终有余额，恶意交易方就能一直通过该攻击提走对方余额。

#### 4.2.5 长程攻击

长程攻击（long range attack）一般出现在使用权益证明（PoS, proof of stake）[69]共识机制算法的区块链网络中，在此类区块链网络中，攻击者如果想要篡改账本，必须拥有至少 51%的算力，这显然难以实现，为达到该目的，恶意节点会先计算生成大量的区块，然后集中一次性放出，以建立一条从区块链第一个区块开始的最长区块链分支，根据区块链最长链原则，新链替换原先合法主链成为新的主链，原主链上已经完成的跨链交易被撤销[70]，从而导致跨链交易可能被双花，攻击者篡改账本的目的达成。

#### 4.2.6 重放攻击

重放攻击（replay attack）[71]是一种恶意重复有效数据传输的网络攻击方式，是指攻击者向目的主机发送一个已被接收过的用于验证用户身份的包，以达到对目的主机进行欺骗攻击的目的，主要用于用户身份认证[72]过程。跨链过程中的重放攻击通常发生在区块链进行硬分叉[73]的时候，硬分叉之后，区块链网络会出现新链+原链的双链状态，由于两条链在交易信息、私钥等方面完全相同，使得一条链上的交易如果出现在另一条链上是完全可行的，这就导致攻击者可能会将一条链上的交易在另一条链上进行恶意重复广播，从而得到确认，这就导致在两条链上完成了两笔相同的交易。

## 5 跨链挑战与展望

### 5.1 挑战

随着以比特币为代表的数字货币的快速发展，

群币崛起、多链共存将会是未来长期的发展局面，虽然现有跨链技术已促进了区块链生态的显著发展，但总体来说，现有跨链技术仍处于起步探索阶段，尚未形成成熟的体系架构，在其技术发展方面还面临着诸多的问题需要解决。

一方面，现有跨链技术由于存在多种不足，难以达到大规模落地应用的需求，例如跨链交易执行效率低的问题[73]、针对恶意行为的预警和处置问题[22]、连接机制的去中心化问题[74]、跨链安全性问题等，都是跨链技术当前及未来发展过程中不可避免的问题，尤其是上文提到的跨链技术难点问题，虽然现有跨链机制能够在一定程度上对其进行解决，但并非完全解决，例如，哈希锁定虽然实现了跨链交易的原子性，但对于某些特殊情况如存在链超时等则无法实现，因此难以保证跨链交易的绝对原子性，再如，通过智能合约模式以及侧链机制中的托管模式可以实现跨链交易资产管理，但由于托管模式相对依赖中心化的托管人以及不是所有区块链系统都支持智能合约等因素[26]，导致其使用范围受限，不能满足所有的需求场景，因此要完全实现跨链交易资产管理还有待技术上的进一步创新突破。

另一方面，跨链技术未来可能面临更加复杂的应用场景，能够适配各类区块链的跨链技术实现难度较大，要想实现全球区块链的广泛互联，需要形成统一的跨链标准和体系。

### 5.2　前景

当前，区块链凭借其独有的信任机制，成为全球范围内新一轮科技革命、产业变革及数字化革命发展的前沿阵地，正在不断改变物联网、数字金融、智能制造等诸多行业的应用场景和运行规则，是未来发展数字经济、构建新型信任体系不可或缺的关键技术，全球多国已将区块链技术应用上升到国家战略层面。为促使区块链技术应用的全球化发展，跨链技术将打破各个区块链应用各自为营的孤立状态，实现跨区块链的价值互通，而跨链技术也必将随着区块链技术的深入发展而不断变革创新。未来跨链技术需要进一步研究的方向包括以下方面。

1) 在公证人机制中，由于引入了受信的第三方，尽管已有较为成熟的选举策略，但跨链交易需要依赖第三方公证人的诚实性，中心化风险较高，虽然多签名公证人机制和分布式签名公证人机制在一定程度上提高了其安全性，但并未完全解决中心化依赖问题，未来，公证人机制可研究结合其他技术如哈希锁定机制[32]等，以进一步增强跨链交互的安全性。

2) 在侧链/中继机制中，由于使用 SPV 证明的区块头部信息对主侧链交易进行支付验证，进行交互的区块链数量不断增多，其带来的开销将对系统处理跨链交易的性能带来影响，此外，由于只通过区块头进行交易验证，无法达到主链对全部交易数据的验证，因此容易遭受双花等恶意攻击，针对诸如此类情况所导致的跨链交易运行效率低、跨链交易存在安全性问题以及中心化风险等问题，未来，一方面可以研究通过主链保存交易记录，侧链存放相关应用代码及数据来缓解主链负担，同时通过优化主侧链的索引机制和跨链交互机制，来进一步提高交易运行效率；另一方面可研究通过多条侧链并行处理来实现交易数据的去中心化，从而提高系统的安全性。

3) 在哈希锁定机制中，针对跨链交易只能实现资产交换而无法实现资产转移的问题，未来可以研究结合公证人机制、侧链机制来实现跨链资产的转移[45]，另外，对于哈希锁定中可能存在的链超时情况导致系统阻塞，增加用户资产被盗风险的问题，未来需要在时间无关性等方面开展深入研究，使得哈希锁定能实现跨链交易的绝对原子性。

4) 在分布式私钥控制机制中，如何降低智能合约的开发难度，且进一步缩减跨链交易等待原链的确认时间以提高运行效率，是未来需要重点研究的方向。而在公证人+侧链混合机制中，未来则需要重点解决作为公证人的分布式节点可能存在共谋风险而无法实现完全去中心化的问题。

5) 针对跨链中恶意行为的预警和处置问题，未来可以考虑从 3 个方面开展研究：一是建立安全可行的节点准入和审计机制；二是要让恶意节点对于网络攻击所付出的成本高于攻击所获得的收益；三是通过建立完善的奖惩机制[61]来激励诚实节点举报恶意节点，并对恶意节点的不端行为进行纠正。

6) 随着应用场景的日趋丰富和复杂化，应对全场景的跨链协议的研究越发重要，未来，跨链可能不会形成一种统一通用的技术，很可能会出现多种跨链技术并存的局面，形成链联网[75]的 TCP/IP 体系，由各种跨链技术提供不同的接口，方便不同区块链选择，以便实现真正的万链互联。

相信不久的将来，随着跨链技术瓶颈逐步被突破，基于跨链机制的互联、高效、安全、可信的区块链技术必将推动人类社会迈向万物互联的新时代，塑造更具前景的社会发展空间。

## 参考文献：


[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Decentralized Business Review, 2008: 21260.

[2] ZHENG Z B, XIE S A, DAI H N, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]//Proceedings of 2017 IEEE International Congress on Big Data (BigData Congress). Piscataway: IEEE Press, 2017: 557-564.

[3] WANG H M, ZHENG Z B, XIE S A, et al. Blockchain challenges and opportunities: a survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352-375.

[4] YAGA D, MELL P, ROBY N, et al. Blockchain technology overview[EB]. 2019.

[5] PILKINGTON M. Blockchain technology: principles and applications[M]//Research handbook on digital transformations. Edward Elgar Publishing, 2016.

[6] 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.
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.

[7] 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.
HE H W, YAN A, CHEN Z H. Survey of smart contract technology and application based on blockchain[J]. Journal of Computer Research and Development, 2018, 55(11): 2452-2466.

[8] 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2018, 44(11): 2011-2022.
YUAN Y, NI X C, ZENG S, et al. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11): 2011-2022.

[9] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[10] WOOD G. Ethereum: a secure decentralised generalised transaction ledger[J]. Ethereum Project Yellow Paper, 2014: 1-32.

[11] GUÉGAN D. Public blockchain versus private blockhain[EB]. 2017.

[12] 吴振铨, 梁宇辉, 康嘉文, 等. 基于联盟区块链的智能电网数据安全存储与共享系统[J]. 计算机应用, 2017, 37(10): 2742-2747.
WU Z Q, LIANG Y H, KANG J W, et al. Secure data storage and sharing system based on consortium blockchain in smart grid[J]. Journal of Computer Applications, 2017, 37(10): 2742-2747.

[13] HAO Y, LI Y, DONG X H, et al. Performance analysis of consensus algorithm in private blockchain[C]//Proceedings of 2018 IEEE Intelligent Vehicles Symposium. Piscataway: IEEE Press, 2018: 280-285.

[14] HOPE-BAILIE A, THOMAS S. Interledger: creating a standard for payments[C]//Proceedings of WWW '16 Companion: Proceedings of the 25th International Conference Companion on World Wide Web. 2016: 281-282.

[15] NOLAN T. Alt chains and atomic transfers[C]//Bitcoin Forum. 2013.

[16] BACK A, CORALLO M, DASHJR L, et al. Enabling blockchain innovations with pegged sidechains[EB]. 2014.

[17] POON J, DRYJA T. The bitcoin lightning network: scalable off-chain instant payments[J]. 2016.

[18] Hyperledger[EB]. 2019.

[19] DILLEY J, POELSTRA A, WILKINS J, et al. Strong federations: an interoperable blockchain solution to centralized third-party risks[EB]. 2016.

[20] KWON J, BUCHMAN E. Cosmos whitepaper[EB]. 2020.

[21] WOOD G. Polkadot: vision for a heterogeneous multi-chain framework[EB]. 2017.

[22] 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 S, HUANG X N, CHEN X L. 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.

[23] 刘懿中, 刘建伟, 张宗洋, 等. 区块链共识机制研究综述[J]. 密码学报, 2019, 6(4): 395-432.
LIU Y Z, LIU J W, ZHANG Z Y, et al. Overview on blockchain consensus mechanisms[J]. Journal of Cryptologic Research, 2019, 6(4): 395-432.

[24] HERLIHY M. Atomic cross-chain swaps[C]//PODC '18: Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing. 2018: 245-254.

[25] BUCHMAN E. Tendermint: Byzantine fault tolerance in the age of blockchains[EB]. 2016.

[26] TEUTSCH J, REITWIEßNER C. A scalable verification solution for blockchains[J]. arXiv preprint arXiv: 1908.04756, 2019.

[27] 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(8): 83-90.
LU A T, ZHAO K, YANG J Y, et al. Research on cross-chain technology of blockchain[J]. Netinfo Security, 2019(8): 83-90.

[28] 章振海, 虞思城, 蒋云杰, 等. 基于区块链交易验证的设备认证方法[J]. 信息安全研究, 2021, 7(6): 550-557.
ZHANG Z H, YU S C, JIANG Y J, et al. Device authentication method based blockchain transaction verification[J]. Journal of Information Security Research, 2021, 7(6): 550-557.

[29] 李强, 颜浩, 陈克非. 安全多方计算协议的研究与应用[J]. 计算机科学, 2003(8): 52-55.
LI Q, YAN H, CHEN K F. Research and application of secure multi-party computation protocols[J]. Computer Science, 2003(8): 52-55.

[30] PALLETONE. Protocol for abstract-level ledger ecosystem[EB]. 2020.

[31] 王劲松, 杨唯正, 赵泽宁, 等. 基于有向无环图的区块链技术综述[J]. 计算机工程, 2022, 48(6): 11-23.
WANG J S, YANG W Z, ZHAO Z N, et al. Survey of directed acyclic graph based blockchain technology[J]. Computer Engineering, 2022, 48(6): 11-23.

[32] 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 page rank algorithm[J]. Computer Engineering, 2021, 47(2): 26-31.

[33] 蒋楚钰, 方李西, 章宁, 等. 基于公证人组的跨链交互安全模型[EB]. 2022.
JIANG C Y, FANG L X, ZHANG N, et al. Cross-chain interaction safety model based on notary mechanism[EB]. 2022.

[34] ASGAONKAR A, KRISHNAMACHARI B. Solving the buyer and seller's dilemma: a dual-deposit escrow smart contract for provably

cheat-proof delivery and payment for a digital good without a trusted mediator[C]//Proceedings of 2019 IEEE International Conference on Blockchain and Cryptocurrency. Piscataway: IEEE Press, 2019: 262-267.

[35] 李尚公, 沈春晖. 资产证券化的法律问题分析[J]. 法学研究, 2000, 22(4): 19-30.
LI S G, SHEN C H. Analysis on the legal issues of asset securitization[J]. Cass Journal of Law, 2000, 22(4): 19-30.

[36] 杨保华, 陈昌. 区块链原理、设计与应用[M]. 2 版. 北京: 机械工业出版社, 2020.
YANG B H, CHEN C. The principle, design and application of blockchain[M]. Beijing: China Machine Press, 2020.

[37] FRIEDENBACH M. Compact spv proofs via block header commitments[J]. 2014.

[38] 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.
CHEN W L, ZHENG Z B. Blockchain data analysis: a review of status, trends and challenges[J]. Journal of Computer Research and Development, 2018, 55(9): 1853-1870.

[39] ETHEREUM. Welcome to BTC relay's documentation[EB]. 2020.

[40] KWON J. Tendermint: Consensus without mining[J]. Draft v. 0.6, fall, 2014, 1(11).

[41] 云闯. 基于侧链技术的区块链可扩展性研究[D]. 天津: 天津大学, 2018.
YUN C. Research on blockchain scalability based on sidechain technology[D]. Tianjin: Tianjin University, 2018.

[42] 刘晶, 朱炳旭, 梁佳杭, 等. 基于主侧链合作的区块链访问控制策略[J]. 计算机工程, 2022, 48(3): 10-16, 22.
LIU J, ZHU B X, LIANG J H, et al. Blockchain access control strategy based on mainchain and sidechain cooperation[J]. Computer Engineering, 2022, 48(3): 10-16, 22.

[43] BEZ M, FORNARI G, VARDANEGA T. The scalability challenge of ethereum: an initial quantitative analysis[C]//Proceedings of 2019 IEEE International Conference on Service-Oriented System Engineering. Piscataway: IEEE Press, 2019: 167-176.

[44] 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.
ZHANG S T, QIN B, ZHENG H B. Research on the protocol of multiple cross-chains based on the hash lock[J]. Cyberspace Security, 2018, 9(11): 57-62, 67.

[45] 李祖建. 基于哈希时间锁定协议的区块链跨链算法研究与应用[D]. 郑州: 郑州大学, 2020.
LI Z J. Research and application of block chain cross chain algorithm based on hashed timelock protocol[D]. Zhengzhou: Zhengzhou University, 2020.

[46] 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.

[47] GENNARO R, JARECKI S, KRAWCZYK H, et al. Secure distributed key generation for discrete-log based cryptosystems[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Heidelberg: Springer-Verlag, 1999: 295-310.

[48] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[49] BLAKLEY G R. Safeguarding cryptographic keys[C]//Managing Requirements Knowledge, International Workshop on. IEEE Computer Society, [S.l.:s.n], 1979: 313-313.

[50] 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.
LIU G H. The cross-chain mechanism of blockchain based on notary group[D]. Chongqing: Chongqing University of Posts and Telecommunications, 2020.

[51] 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.

[52] 王兵, 李辉灵, 牛新征. 基于综合选举的 DPoS 共识算法[J]. 计算机工程, 2022, 48(6): 50-56.
WANG B, LI H L, NIU X Z. DPoS consensus algorithm based on comprehensive election[J]. Computer Engineering, 2022, 48(6): 50-56.

[53] 孙国梓, 王纪涛, 谷宇. 区块链技术安全威胁分析[J]. 南京邮电大学学报(自然科学版), 2019, 39(5): 48-62.
SUN G Z, WANG J T, GU Y. Security threat analysis of blockchain technology[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2019, 39(5): 48-62.

[54] 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.

[55] 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.

[56] 斯雪明, 徐蜜雪, 苑超. 区块链安全研究综述[J]. 密码学报, 2018, 5(5): 458-469.
SI X M, XU M X, YUAN C. Survey on security of blockchain[J]. Journal of Cryptologic Research, 2018, 5(5): 458-469.

[57] MOHURLE S, PATIL M. A brief study of wannacry threat: ransomware attack 2017[J]. International Journal of Advanced Research in Computer Science, 2017, 8(5): 1938-1940.

[58] 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.
CAI X Q, DENG Y, ZHANG L, et al. The principle and core technology of blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 84-131.

[59] 胡旭骏. 区块链技术在政务网络身份凭证中心的应用研究: 以 XX 市为例[D]. 昆明: 云南财经大学, 2020.
HU X J. Research on the application of block chain technology in government affairs network identity certificate center—A case study of XX city[D]. Kunming: Yunnan University of Finance and Economics, 2020.

[60] 邸剑, 吝伟华. 区块链中矿池选择策略的研究与分析[J]. 计算机应用研究, 2020, 37(6): 1804-1807.
DI J, LIN W H. Research and analysis of mining pool selection strategy in blockchain[J]. Application Research of Computers, 2020, 37(6): 1804-1807.

[61] 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.

[62] ROSENFELD M. Analysis of hashrate-based double spending[EB]. 2014.

[63] 孙浩, 毛瀚宇, 张岩峰, 等. 区块链跨链技术发展及应用[J]. 计算机科学, 2022, 49(5): 287-295.
SUN H, MAO H Y, ZHANG Y F, et al. Development and application of blockchain cross-chain technology[J]. Computer Science, 2022, 49(5): 287-295.

[64] HEILMAN E, KENDLER A, ZOHAR A , et al. Eclipse attacks on Bitcoin's peer-to-peer network[C]//USENIX Security Symposium, USENIX Association. [S.l.:s.n], 2015.

[65] MARCUS Y, HEILMAN E, GOLDBERG S. Low-resource eclipse attacks on ethereum's peer-to-peer network[J]. Cryptology ePrint Archive, 2018.

[66] DOUCEUR J R. The sybil attack[C]//International workshop on peer-to-peer systems. Heidelberg: Springer-Verlag, 2002: 251-260.

[67] 张志威, 王国仁, 徐建良, 等. 区块链的数据管理技术综述[J]. 软件学报, 2020, 31(9): 2903-2925.
ZHANG Z W, WANG G R, XU J L, et al. Survey on data management in blockchain systems[J]. Journal of Software, 2020, 31(9): 2903-2925.

[68] 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.

[69] 韩璇, 刘亚敏. 区块链技术中的共识机制研究[J]. 信息网络安全, 2017(9): 147-152.
HAN X, LIU Y M. Research on the consensus mechanisms of blockchain technology[J]. Netinfo Security, 2017(9): 147-152.

[70] GREEN M, MIERS I. Bolt: anonymous payment channels for decentralized currencies[C]//Proceedings of CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017: 473-489.

[71] SONNINO A, BANO S, AL-BASSAM M, et al. Replay attacks and defenses against cross-shard consensus in sharded distributed ledgers[C]//Proceedings of 2020 IEEE European Symposium on Security and Privacy (EuroS&P). Piscataway: IEEE Press, 2020: 294-308.

[72] 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. Survey on identity management in blockchain[J]. Journal of Software, 2021, 32(7): 2260-2286.

[73] 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.
HAN X, YUAN Y, WANG F Y. Security problems on blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2019, 45(1): 206-225.

[74] 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.

[75] 孟博, 王乙丙, 赵璨, 等. 区块链跨链协议综述[EB]. 2022.
MENG B, WANG Y B, ZHAO C, et al. Survey on cross-chain protocols of blockchain[EB]. 2022.

[作者简介]

**沈传年**（1981– ），男，国家计算机网络应急技术处理协调中心上海分中心工程师，主要研究方向为网络与信息安全、区块链等。