

## 基于混合链结构的隐私保护交易系统监管方案

贾雪丹<sup>1,2</sup>, 黄龙霞<sup>1</sup>, 经普杰<sup>1</sup>, 王良民<sup>3</sup>, 宋香梅<sup>1</sup>

(1. 江苏大学计算机科学与通信工程学院, 江苏 镇江 212013;

2. 江苏省食品质量安全重点实验室-国家重点实验室培育基地, 江苏 南京 210014; 3. 东南大学网络空间安全学院, 江苏 南京 211189)

**摘要:** 区块链技术因其去中心化、透明性和安全性等特点, 广泛应用于金融、物联网和供应链等行业。但区块链技术的应用在带来行业变革机会的同时, 给行业监管带来了新的挑战。一方面, 传统中心化监管手段会破坏区块链去中心化和自治性的可信基础, 导致区块链应用系统面临监管困境; 另一方面, 区块链应用系统存在隐私保护需求, 交易中通常包含比货币数量更多的敏感信息, 交易暴露会直接导致隐私泄露。区块链应用系统隐私保护会增加监管部门对交易情况的监管难度。针对隐私保护的区块链交易系统监管需求, 提出基于混合链结构的监管方案, 设计了基于多委员会的通用跨链协作监管方法; 设置监管链和业务链监管委员会, 通过业务链监管委员会对业务链信息产生隐私保护的证明, 进而实现隐私保护的监管; 在链内交易监管的同时, 通过跨链通信委员会和监管委员会共同实现对业务链之间的跨链交易监管。根据监管方案的安全需求, 证明了当每个组件满足其安全要求时, 监管方案是安全的。为了验证方案的可行性, 用有效组件实现, 并进行实验评估。结果表明, 所提方案以较低的成本实现了跨链监管, 并具有通用性和可扩展性。

**关键词:** 区块链; 监管; 跨链; 隐私

**中图分类号:** TP393

**文献标志码:** A

**DOI:** 10.11959/j.issn.2096-109x.2023083

## Hybrid-chain-based supervision scheme for privacy-preserving trading system

JIA Xuedan<sup>1,2</sup>, HUANG Longxia<sup>1</sup>, JING Pujie<sup>1</sup>, WANG Liangmin<sup>3</sup>, SONG Xiangmei<sup>1</sup>

1. School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China

2. Jiangsu Key Laboratory for Food Quality and Safety-State Key Laboratory Cultivation Base, Nanjing 210014, China

3. School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China

**收稿日期:** 2023-08-14; **修回日期:** 2023-10-23

**通信作者:** 王良民, liangmin@seu.edu.cn

**基金项目:** 国家重点研发计划(2022YFD2100605); 国家自然科学基金(62102168); 江苏省前沿引领技术基础研究专项(BK20202001); 江苏省自然科学基金(BK20200888)

**Foundation Items:** The National Key R&D Program of China (2022YFD2100605), The National Natural Science Foundation of China (62102168), The Leading-Edge Technology Program of Jiangsu Natural Science Foundation (BK20202001), The Natural Science Foundation of Jiangsu Province (BK20200888)

**引用格式:** 贾雪丹, 黄龙霞, 经普杰, 等. 基于混合链结构的隐私保护交易系统监管方案[J]. 网络与信息安全学报, 2023, 9(6): 56-70.

**Citation Format:** JIA X D, HUANG L X, JING P J, et al. Hybrid-chain-based supervision scheme for privacy-preserving trading system[J]. Chinese Journal of Network and Information Security, 2023, 9(6): 56-70.

**Abstract:** Due to its characteristics of decentralization, transparency, and security, blockchain technology is widely used in finance, the Internet of Things, and supply chain. However, along with the opportunities it brings, the application of blockchain technology also presents new challenges. On one hand, traditional centralized regulatory methods can undermine the decentralized and autonomous nature of blockchain, creating regulatory dilemmas. On the other hand, blockchain-based systems require privacy protection as transactions often contain sensitive information beyond currency amounts. Failure to protect privacy can result in information leakage and make it difficult for authorities to monitor transactions. To address these challenges and enable regulation in privacy-preserving blockchain-based trading systems, a hybrid chain framework was proposed. This framework incorporated a multiple committee-based approach for general cross-chain regulation. Separate committees were established for the supervision chain and service chain. The service chain committee handled service chain data, generating and sending proofs to the supervision chain to achieve private supervision. In addition to single-chain regulation, cross-chain communication committees and supervision committees collaborated to achieve cross-chain transaction supervision among different service chains. Through a security analysis, it is proven that the proposed scheme is secure when each module meets its security requirements. Experimental evaluations have been conducted to demonstrate the feasibility of the proposed scheme, showing that it achieves cross-chain supervision at a low cost and is scalable.

**Keywords:** blockchain, supervision, cross-chain, privacy

## 0 引言

区块链是以密码学算法为基础的点对点分布式账本技术,允许交易以去中心化的方式进行<sup>[1]</sup>。自比特币诞生以来,区块链技术迅速发展,区块链数量不断增长,截至2022年,基于区块链的“加密货币”超过1万种<sup>[2]</sup>。区块链技术因其去中心化、透明性和安全性等特点,广泛应用于金融科技<sup>[3-4]</sup>、公共服务<sup>[5]</sup>、物联网<sup>[6-7]</sup>和供应链<sup>[8]</sup>等领域。虽然多数应用领域,如“加密货币”、金融科技和供应链等,更青睐公共区块链,但在其他应用领域,如企业计算和医疗保健等,寻求采用许可区块链。不同种类的区块链系统产生了区块链互操作需求,即在不改变底层区块链系统的条件下,在公共区块链和许可区块链之间,实现灵活资产转移、数据共享和智能合约调用<sup>[9]</sup>。

异构区块链生态系统的发展为系统安全带来更大挑战。虽然区块链技术在分布式场景下,为各种应用提供可信执行环境和可靠数据来源,增加了系统的安全性和透明性。但众多异构区块链并存给系统带来区块链互操作难题。首先,异构区块链基础设施使用不同加密原语,如数字签名方案和哈希算法,增加了异构区块链之间的互操作难度。如果两条链采用不同签名方案,很难实现跨链协议<sup>[10]</sup>。其次,区块链技术面临的监管困

境在异构区块链系统中表现更为突出。目前已提出一些区块链监管技术:数字交易监管、链下监管和接入式监管<sup>[11]</sup>。数字交易监管通过网络层节点检测、交易层数据分析和应用层网络流量分析,发现和追踪“数字货币”交易中的恶意节点、可疑交易和异常用户。链下监管指对上链前的交易和合约数据进行链下审计和检测,但通过上链审查后,就难以对链上数据和行为进行控制,且链下监管多采用中心化思想,在一定程度上破坏了区块链技术的去中心化和透明性。接入式监管将监管实体作为区块链节点,参与区块链业务并获取数据,实现区块链数据和行为监管。然而,这些监管方法不涉及区块链技术本身,或者可能破坏区块链系统的隐私性和去中心化,引起区块链用户对系统安全的担忧。区块链监管仍面临两方面的难题:一方面,区块链去中心化、自治性的可信基础与传统的中心化监管手段存在本质冲突,中心化监管会破坏基于区块链技术构建可信系统的意义;另一方面,区块链交易系统存在隐私保护需求。研究表明,即使用户只使用公钥和私钥进行交易,区块链也可能发生隐私泄露<sup>[12-14]</sup>。交易中通常包含除了货币数量之外更多的敏感信息,如位置、数据访问模式等,交易暴露会导致用户隐私信息泄露,进一步造成更大危害。区块链交易系统隐私保护增加了监管部门对交易情况

的监管难度。

针对隐私保护的区块链交易系统监管需求,本文提出基于混合链结构的监管架构,设计了基于多委员会的通用跨链协作监管方法;设置不对称的监管链和业务链监管委员会,通过业务链监管委员会对业务链信息产生隐私保护的证明,实现监管链对业务链的隐私保护的单向监管。在链内交易监管同时,通过设置对称的跨链通信委员会,实现双向跨链交易,且由非对称的监管委员会实现业务链间跨链交易的监管。本文工作主要包括以下3个方面。

1) 提出基于混合链的监管架构,分为监管层、跨链层和业务层。监管层包含监管规则、监管者联盟和监管链;跨链层由跨链委员会实现跨链监管和跨链交易;业务层包含多条基于异构区块链的业务链。该架构实现了监管链根据监管规则对业务链内部和业务链之间的交易监管,通过模块化设计,实现了不同用例和功能,包括跨链监管和跨链交易。

2) 所提架构中的跨链层采用委员会机制实现跨链监管和跨链交易。针对基于委员会的跨链系统中多数诚实假设带来的跨链安全性低和单点故障问题,本文提出基于多委员会和零知识证明的跨链方法,实现无许可和去中心化的跨链交易和跨链监管,无须引入严格的信任假设,只要监管链和业务链委员会各存在一个诚实节点,跨链监管就可以安全执行,且跨链委员会成员通过选举组件定期更新,防止固定成员受到贿赂攻击,保障跨链安全性。

3) 验证了所提方案的安全性和有效性。基于Fabric搭建不同区块链,并用委员会节点连接区块链网络,进行实验评估。结果表明,所提方案以较低的成本实现了跨链监管,并具有通用性和可扩展性。

## 1 相关工作

### 1.1 跨链技术

区块链跨链技术是提升区块链间互操作性,解决区块链间数据共享困难的重要保障<sup>[15]</sup>。学者已经提出多种方案来解决区块链之间的互操作和数据共享问题<sup>[16]</sup>,包括公证人机制、侧链/中继、

哈希锁定和分布式私钥控制等<sup>[17]</sup>技术方案,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和信息的流通。

公证人机制通过引入可信第三方进行跨链消息转发和验证,相对容易实现。Tian等<sup>[18]</sup>提出一种使用去中心化公证方案的“加密货币”交换协议,随机选择不受信任的中介,加入验证委员会来转发和验证交易,并通过智能合约确保公证人的正确行为。Shao等<sup>[19]</sup>结合公证人和代理节点,提出基于身份加密的物联网区块链跨链通信机制,实现代理节点之间的直接跨链通信和通过公证人的间接跨链通信。Zhang等<sup>[20]</sup>提出一种基于委员会的通用跨链转账方案,并保证了跨链原子性和终止性。文献[21]提出一个两阶段跨链模型(公证人转移跨链交易请求,公证人作为中间人转移资产),为了避免单点故障,提出基于组的公证人模型和公证人选择机制,从公证人组中选择一个公证节点来处理跨链交易。但是,公证人方案存在依赖可信第三方导致安全性较弱的问题。

本文方案采用跨链委员会实现跨链交易和跨链监管,不同于当前基于公证人和委员会的方案,委员会成员无须在两条区块链拥有账户以获取交易数据,且结合零知识证明,实现隐私保护的跨链监管和跨链交易。

### 1.2 跨链监管

随着“加密货币”和区块链技术的应用发展,各国已经注意到区块链监管的重要性,但多数国家更加注重对“加密货币”的监管,对区块链技术本身的监管保持着审慎的态度<sup>[22]</sup>。中国工程院院士陈纯在2019 CCF区块链技术大会上发表了“联盟区块链关键技术与区块链的监管挑战”主题演讲,提出了用区块链技术治理区块链及其应用的思想。

Wang等<sup>[23]</sup>将区块链安全监管关键技术分为3个方面:网络层的节点发现技术、交易层的交易记录数据分析技术和应用层的网络流量分析技术。经普杰等<sup>[11]</sup>提出了一种分层跨链的监管架构,设计了“监管链-业务链”跨链协作的监管模式;设置策略层和监管层、业务层,分离监管行为和监管技术,构建去中心化监管链,改善监管集权,实现了通用的区块链监管结构。

针对不同应用场景中的监管问题,学者已提出针对性解决方案。余春堂等<sup>[24]</sup>提出基于区块链的众包物流分级监管架构,实现了智能交易匹配、异常数据检测与分析等功能,并在众包物流企业平台上进行测试,证明架构的可行性。针对传统食品监管体系中产业链缺失和数据碎片化问题,Tao 等<sup>[25]</sup>提出了分级多域区块链网络结构和二次检查机制,支持区域节点共治并及时纠正和替换恶意监管节点,实现监管节点辅助验证以及上级区域仲裁。针对模块化住房生产中的监管问题,Li 等<sup>[26]</sup>提出基于区块链的两层自适应监管模型(参与者自适应私有侧链和用于所有参与者通信和交易的主区块链),避免了主区块链对运营记录的篡改。为了保证大米食品质量安全,Peng 等<sup>[27]</sup>提出了一种基于多层区块链的大米供应链精细化监管模型,通过分析大米供应链中信息流的特点,构建了关键信息的分类表,实现了大米供应链中的各类数据精细化监管。针对集中式电子商务评价系统存在的欺诈和操纵问题,Wang 等<sup>[28]</sup>构建基于以太坊智能合约的评价审查系统,通过代理查询供应链系统中购买者的身份,并由智能合约验证新的评论,保证评论的可靠性和不易篡改。

不同于上述针对特定应用环境的监管方案,本文设计基于混合链结构和多委员会的跨链交易系统通用监管方案,通过不对称委员会设置,并结合零知识证明,实现隐私保护的跨链监管。

## 2 预备知识

本节介绍区块链和零知识证明的相关知识。

### 2.1 区块链

从技术上看,区块链是一种可信、不易篡改的数据结构。每个区块都经过共识上链,包含前一个块的哈希值、块的哈希值、时间戳、事务和其他信息。哈希函数由于防碰撞的特点,很难对已经确认的区块进行修改。区块链分为公链、私链和联盟链。许多区块链系统支持智能合约,智能合约是通过交易发布在区块链上的有状态程序。用户通过发送交易与合约交互,并可能更改合约状态。现有智能合约平台面临的关键限制是计算和存储资源,导致链上开销昂贵。在区块链网络中,既有完整节点,又有轻节点。完整节点

存储区块链所有历史数据,同时可以验证区块头和所有交易;而轻节点只存储区块头,其工作由底层的共识协议决定。

### 2.2 零知识证明

零知识证明是指证明者能够在不向验证者提供任何隐私信息的情况下,使验证者相信论断是正确的。零知识证明是包含密钥生成、证明和验证的多项式时间算法 $(G, P, V)$ <sup>[29]</sup>。针对密钥生成算法 $G$ ,给定一个安全参数和一个 $F$ -运算电路,产生证明密钥 $pk$ 和验证密钥 $vk$ 。之后,证明者可以使用 $pk$ 生成非交互式证明 $\pi$ ,验证者可以使用 $vk$ 来检查证明 $\pi$ 。即给定证明密钥 $pk$ 和任意输入 $x$ ,存在 $w$ 满足 $(x, w) \in R$ ,证明者通过 $P(pk, x, w)$ 产生证明 $\pi$ ;验证者通过 $V(vk, x, \pi)$ 检查 $\pi$ 是否为 $x$ 的有效证明<sup>[10]</sup>。

## 3 基于混合链的监管方案

本文提出基于混合链的监管方案,包括业务链、监管链和跨链委员会。系统用户包括业务链 $Pch1$ 付款人 $A$ 、业务链 $Pch2$ 收款人 $B$ 和监管链监管者联盟。 $A$ 作为跨链交易发起方,转账给 $Pch2$ 的用户 $B$ ,或与 $B$ 做原子交换。监管者联盟通过监管链发布监管规则和监管交易,对业务链自身运行和跨链交易情况进行监管。采用多委员会,即在不同链分别选择不同跨链委员会,委员会成员无须拥有两条链账户,也无须获取两条链数据。委员会采用零知识证明产生证明信息,且成员定期更新,并根据信誉值选择新的委员会。

### 3.1 威胁模型

本文考虑到业务链用户可能恶意破坏链内或跨链交易公平,恶意行为包括恶意付款人可能不进行转账或重复支出;恶意收款人收到转账后骗取额外赔偿。跨链通信包括跨链监管和跨链业务,通过跨链委员会实现,需要满足正确性和及时性。考虑委员会成员可能因为客观或主观因素,导致无法按照协议执行。对委员会成员的安全性假设,本文遵循文献[10],除了底层区块链安全假设之外,不引入额外的信任假设,即假设发送方区块链和接收方区块链是安全的,且发送方区块链有一个轻节点协议来实现快速的区块头验证。基于以上两种属性,本文假设各委员会中至少有一个

诚实节点, 并且使用的零知识证明是健全的。

### 3.2 安全目标

本文旨在设计隐私保护的通用区块链系统监管方案, 设计目标如下。

1) 去中心化: 不基于任何集中式第三方实现跨链, 且协议中的任何一方都不能否认自己的行为。

2) 通用性: 监管框架支持多种类型区块链, 即不受区块链类型的限制。

3) 稳定性: 在安全假设下, 协议能够抵御区块链网络中的常见攻击, 如针对委员会成员的贿赂。

4) 隐私和安全: 监管链在不获取业务链原始数据的情况下验证业务链运行的正确性。针对跨链交易, 监管发起链和接收链跨链行为的完整性, 保证跨链交易的安全性。

### 3.3 监管模型

针对隐私保护的区块链交易系统监管需求, 本节提出一种混合链监管层次架构, 如图1所示。该架构的核心在于在跨链业务的基础上实现跨链监管, 通过多跨链委员会将跨链业务与跨链监管分离, 并实现适用于不同业务链类型的通用监管模型。顶层是监管层, 监管链作为独立模块, 实现对底层业务系统的灵活监管。不同区块链应用系统作为底层独立模块, 执行相应的应用业务逻辑。核心模块是中间层的跨链监管模块和跨链通信模块。为了实现不依赖于特定应用场景和特殊应用类型的区块链通用监管框架, 采用代理节点, 通过选举形成跨链委员会, 并分别构建监管委员会和通信委员会。跨链模块不参与上下层区块链共识过程, 不会影响上下层区块链本身的交易确认和执行。

#### (1) 监管层

在监管层中, 多部门联合设置对业务层不同应用业务的监管联盟, 并通过跨链层的监管模块接入相应业务系统进行监管。监管层根据既定的监管规则, 通过监管委员会定期对业务链行为进行监管验证。首先, 监管链委员会根据监管需求向业务链委员会发起监管请求; 然后, 业务链根据监管指令执行智能合约获取监管所需的数据, 并将数据交给业务链监管委员会进行验证和隐私处理后, 跨链返回给监管链委员会; 监管链委员会

对业务数据进行验证并提交给监管链分析, 如果存在异常业务行为, 监管链对业务链请求进一步监管, 获取更多信息, 进行更细粒度的异常追踪; 最后, 监管链委员会把监管结果写入监管链存档。

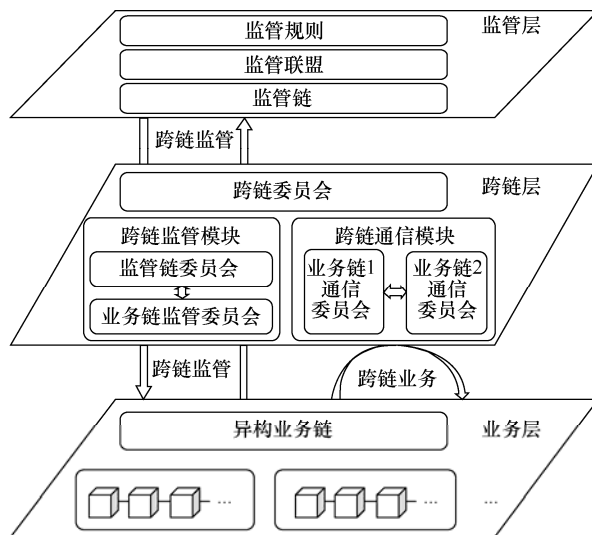


图1 混合链监管层次架构

Figure 1 Hierarchical architecture of hybrid-chain supervision

#### (2) 跨链层

跨链层是执行跨链监管和跨链交互的关键, 主要包括两个模块: 跨链监管模块和跨链通信模块。跨链监管模块主要实现监管层对业务层的跨链监管, 由监管链委员会和业务链监管委员会共同组成, 委员会成员分别由监管链和业务链选举产生, 作为区块链轻节点不参与区块链共识, 主要负责监管信息处理和传递。监管需求传到业务链后, 由业务链监管委员会对业务链数据进行验证和隐私处理, 然后交给监管链委员会, 防止监管链委员会直接获取业务链数据, 破坏业务隐私。跨链通信模块主要负责不同业务链之间的交易和信息传递, 分别由业务链节点选取产生跨链通信委员会, 实现业务链之间隐私保护的跨链价值转移和数据共享。

#### (3) 业务层

业务层包含不同类型的应用区块链, 分别处理不同的业务数据。业务链内通过共识维护链上数据, 保障业务系统内部安全与隐私。不同业务链之间通过上层的跨链通信模块实现多部门、多场景应用系统间的交易、通信和数据共享, 且各条区块链链内业务不受跨链交互层影响。

### 3.4 跨链模块

本节提出基于委员会的跨链模块，跨链模块设计如图2所示。跨链监管模块分为监管链委员会 Cmte\_S 和业务链监管委员会 Cmte\_SP，分别由5个部分组成：监管委员会成员选举（SCE，supervisor committee election）组件、隐私保护证明产生（PPG，privacy-preserving proof generation）组件、隐私保护证明验证（PPV，privacy-preserving proof verification）组件、链间信息传递（IID，inter-chain information delivery）组件和信誉管理（RM，reputation management）组件。因为监管模块考虑监管层对业务层的单向监管，故业务链监管委员会和监管链委员会构成组件略有差异，分别负责业务链的隐私保护证明产生和业务链的隐私保护证明验证。

不同于跨链监管模块，跨链通信模块是对称的，实现业务链之间的双向跨链交易和信息传递。跨链通信模块由业务链1通信委员会 Cmte\_Pch1 和业务链2通信委员会 Cmte\_Pch2 共同构成，分别包括5个部分：通信委员会成员选举（CCE，communication committee election）组件、PPG 组件、PPV 组件、IID 组件和 RM 组件。

为了实现对业务链的交易监管，业务链 Pch1、Pch2 和监管链 S 分别维护自己的跨链通信委员会 Cmte\_Pch1、Cmte\_Pch2 和跨链监管委员会 Cmte\_SP1、Cmte\_SP2 和 Cmte\_S。每个委员会成员拥有其所属链上的一个账户，并运行轻客户端。

通过上述基于委员会的跨链模型，所提方案

实现业务链之间的跨链交易和数据共享，并保证监管链对不同业务链的监管。虽然所提方案基于委员会，但无须引入严格信任假设，只要 Cmte\_SP 和 Cmte\_S 中至少存在一个诚实节点，跨链监管就可以安全执行，实现了无许可和去中心化的跨链通信和监管。跨链委员会成员通过 SCE 组件和 CCE 组件定期更新，防止固定成员受到贿赂攻击。

## 4 协议设计

### 4.1 跨链通信模块

为了实现业务链之间的跨链交互，业务链 Pch1、Pch2 分别维护自己的跨链通信委员会 Cmte\_Pch1、Cmte\_Pch2。本文考虑两种业务链跨链交易模式：跨链转账和跨链原子交换。

#### （1）跨链转账

假设 A 和 B 分别是业务链 Pch1 和 Pch2 用户，A 向 B 发起转账支付交易。跨链转账需要在业务链 Pch1 和 Pch2 跨链通信委员会 Cmte\_Pch1、Cmte\_Pch2 之间进行通信，并由 Cmte\_Pch1、Cmte\_Pch2 进行跨链转账验证和确认。跨链转账协议如图3所示，具体包括跨链转账请求、验证和确认，详细步骤如下。

**Step1 转账请求。**业务链 Pch1 用户 A 需要向业务链 Pch2 用户 B 转账  $b$ ，A 向 Pch1 跨链通信委员会 Cmte\_Pch1 发起转账请求，并在 Pch1 上提交一笔交易  $tr_1^i$ ，锁定转账金额  $b$ 。当该交易被打包上链后，Cmte\_Pch1 向 Pch1 全节点请求获得区块信息，根据 Merkle 树证明对交易包含性进行验证。通过验证之后，Cmte\_Pch1 由 PPG 组件

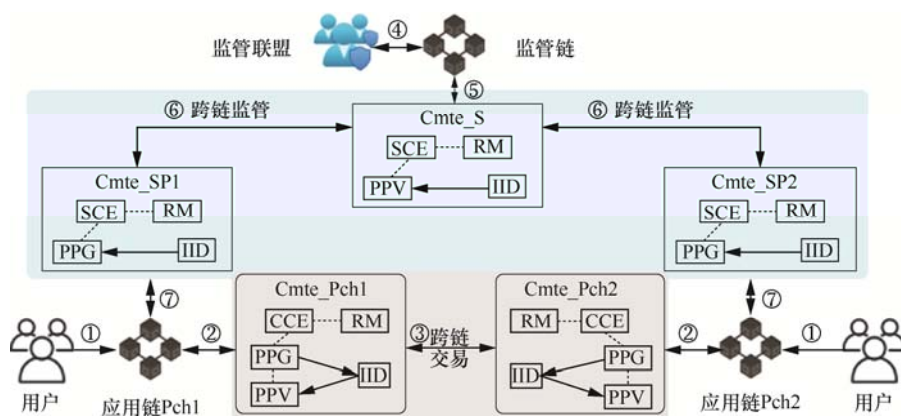


图2 跨链模块设计

Figure 2 Cross chain module design

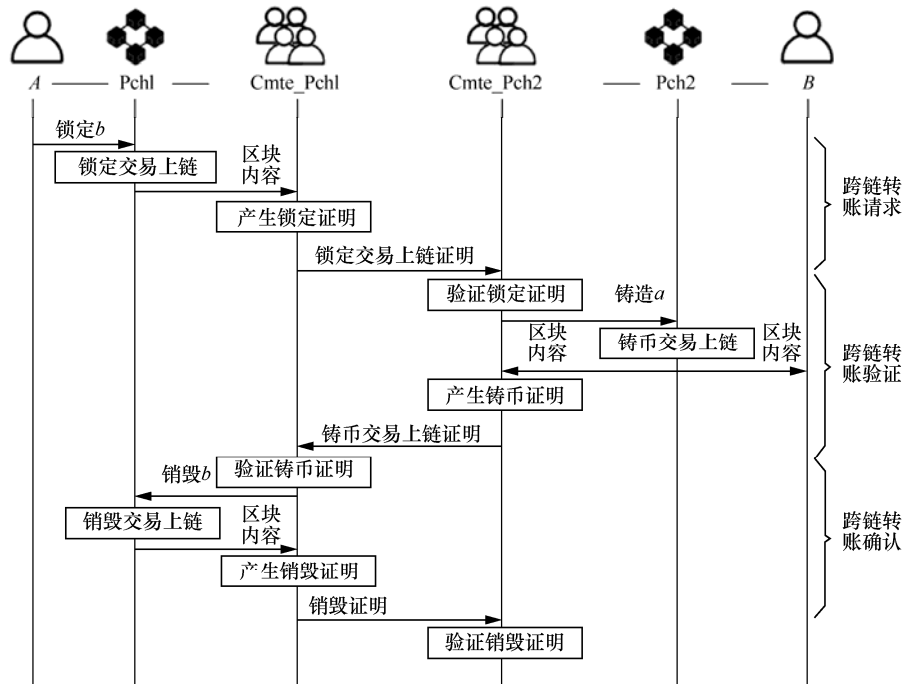


图 3 跨链转账协议

Figure 3 Cross-chain transfer protocol

产生锁定交易  $tr_1^l$  上链的证据  $p_{tr_1^l}$ ，并通过 IID 组件跨链传递给 Cmte\_Pch2。

**Step2 转账验证。**Cmte\_Pch2 的 IID 组件首先接收来自 Cmte\_Pch1 的信息  $p_{tr_1^l}$ ，由 PPV 组件进行验证，确认 A 确实锁定了  $b$  金额；然后通过铸币交易  $tr_2^c$  为 B 账户增加与 A 的转账金额  $b$  等价的  $a$  代币；最后由 Cmte\_Pch2 的 PPG 组件把铸币交易  $tr_2^c$  完成证明  $p_{tr_2^c}$  通过 IID 组件传递给 Cmte\_Pch1 进行确认。

**Step3 转账确认。**Cmte\_Pch1 的 IID 组件接收来自 Cmte\_Pch2 的信息  $p_{tr_2^c}$ ，由 PPV 组件进行验证，确认业务链 Pch2 铸币交易  $tr_2^c$  已经完成；通过交易  $tr_1^d$  把 A 的锁定金额  $b$  销毁；最后 Cmte\_Pch1 产生交易  $tr_1^d$  完成证明  $p_{tr_1^d}$  给 Cmte\_Pch2，验证销毁交易，确认转账完成。否则，Cmte\_Pch1、Cmte\_Pch2 分别执行撤销交易  $tr_1^r$  和  $tr_2^r$ ，来撤销未完成的跨链转账。

## (2) 跨链原子交换

假设 A 向 B 发起跨链原子交换，即 A 用自己在链 Pch1 上的  $b$  代币换取 B 在链 Pch2 上的  $a$  代币，需要在业务链 Pch1 和 Pch2 跨链通信委员会 Cmte\_Pch1、Cmte\_Pch2 之间进行 4 轮跨链通信，

跨链交换协议如图 4 所示，具体跨链交换步骤如下。

**Step1 交易请求。**A 向 Cmte\_Pch1 发起交换请求，并在 Pch1 上提交  $tr_1^l$  锁定转账金额  $b$ ；B 向 Cmte\_Pch2 发起交换请求，并在 Pch2 上提交  $tr_2^l$  锁定  $a$ 。锁定交易上链后，Cmte\_Pch1 和 Cmte\_Pch2 分别向 Pch1、Pch2 全节点请求获得区块信息，并根据 Merkle 树证明对交易包含性进行验证。通过验证之后，Cmte\_Pch1 的 PPG 组件产生交易  $tr_1^l$  上链证据  $p_{tr_1^l}$ ，通过 IID 组件跨链传递给 Cmte\_Pch2；同样，Cmte\_Pch2 产生交易  $tr_2^l$  上链证据  $p_{tr_2^l}$ ，并传递给 Cmte\_Pch1。

**Step2 锁定验证。**Cmte\_Pch2 的 IID 组件接收来自 Cmte\_Pch1 的信息  $p_{tr_1^l}$ ，由 PPV 组件进行交易验证，确认 A 在 Pch1 上锁定了  $b$  金额。同样，Cmte\_Pch1 的 IID 组件接收到  $p_{tr_2^l}$  后，PPV 组件验证交易，确认 B 在 Pch2 上锁定了  $a$  金额。

**Step3 链内转账。**Cmte\_Pch2 确认 A 的锁定，通过 Pch2 共识执行转账  $tr_2^c$ ，将 B 锁定的  $a$  转移到 A 在 Pch2 上的地址，Cmte\_Pch2 的 PPG 组件把  $tr_2^c$  完成证明  $p_{tr_2^c}$  通过 IID 组件传递给 Cmte\_Pch1 进行确认；Cmte\_Pch1 确认 B 锁定  $a$  金

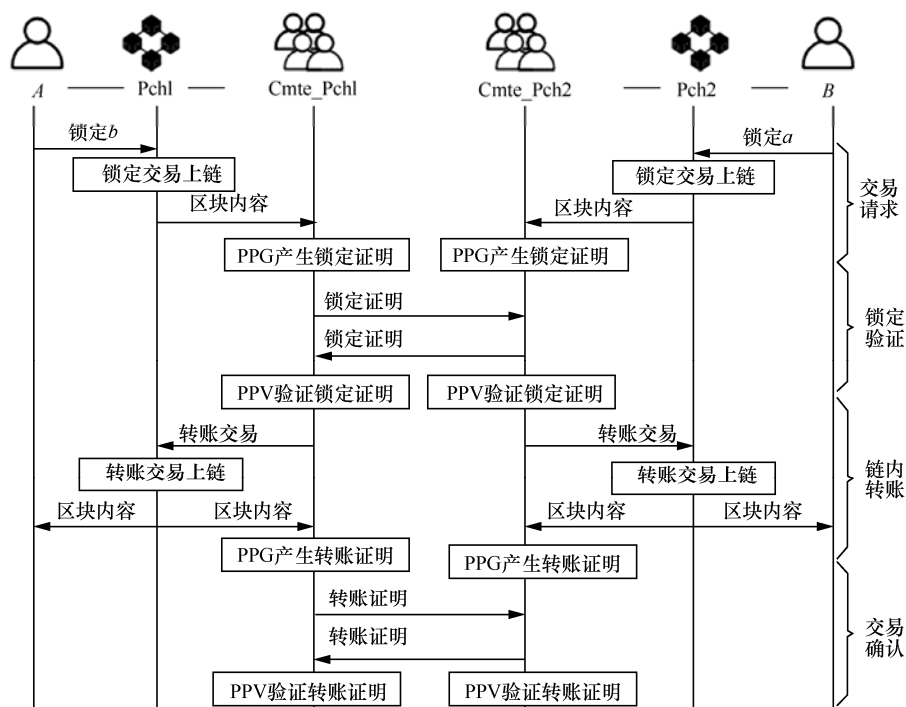


图4 跨链交换协议

Figure 4 Cross-chain exchange protocol

额, 执行交易  $tr_1^2$ , 将 A 锁定的金额  $b$  转移到 B 在 Pchl 上的地址, Cmte\_Pchl 把交易  $tr_1^2$  完成证明  $p_{tr_1^2}$  传递给 Cmte\_Pch2 验证。

**Step4 交易确认。**Cmte\_Pchl 接收  $p_{tr_1^2}$ , 验证 Pch2 转账交易  $tr_2^2$  完成; Cmte\_Pch2 接收  $p_{tr_1^2}$ , 确认 Pchl 完成  $tr_1^2$ 。否则, Cmte\_Pchl、Cmte\_Pch2 分别执行撤销交易  $tr_1^{rs}$  和  $tr_2^{rs}$ , 来撤销未完成的原子交换。

## 4.2 跨链监管模块

为了实现业务链监管, 监管链和业务链 Pchl、Pch2 分别维护自己的跨链监管委员会 Cmte\_S、Cmte\_SP1 和 Cmte\_SP2。委员会成员拥有其所属链上的一个账户, 运行区块链轻客户端。跨链监管协议如图 5 所示。

首先, 监管链根据监管规则发起监管交易, Cmte\_S 根据监管交易中的监管需求, 通过 IID 组件向业务链监管委员会发起监管请求。Cmte\_SP 成员持续跟踪业务链区块头, 根据 Merkle 证明验证交易包含性。然后, 由 PPG 组件基于零知识证明向监管链证明业务链执行的正确性, 并把证明结果通过 IID 组件传递给监管链。Cmte\_S 通过 IID

组件接收到 Cmte\_SP 的证明信息, 由 PPV 组件对证明结果进行验证, 并将验证结果提交到监管链。具体的隐私保护证明产生、隐私保护证明验证和链间信息传递算法如算法 1~算法 3 所示。

### 算法 1 PPG

PPG 组件负责对获取的区块链数据进行验证, 并采用零知识证明对通过验证的区块链数据生成隐私保护的证明。

首先, 从  $k$  个区块链完整节点处获得时间区间  $[t_1, t_2]$  内的区块信息, 即  $B_i, B_{i+1}, \dots, B_k$ , 检查交易的包含性和完整性。

然后, 根据区块头信息生成零知识证明  $\pi = P(pk, B_{i-1}, \dots, B_k, LCS_{i-1})$ , 证明时间区间  $[t_1, t_2]$  内区块  $B_i, B_{i+1}, \dots, B_k$  的正确性。本质上是证明区块头  $BH_i, BH_{i+1}, \dots, BH_k$  在  $BH_{i-1}$  之后被轻客户端接受。根据当前轻客户端状态  $LCS_{i-1}$ , 有  $LightC(LCS_{i-1}, BH_{i-1}, \dots, BH_k) \rightarrow true$  成立。

最后, 根据具体的监管要求, 发送  $(BH_{i-1}, BH_i, \dots, BH_k, Prf_{SP}, \pi)$  到 IID 组件。

为了避免由于委员会成员同时执行上述算法产生冲突而浪费证明时间 (当多个委员会节点同时产生证明信息时, IID 组件只会接收一个证明



激励委员会节点诚实地执行协议。SCE 组件和 CCE 组件根据节点信誉值，定期进行委员会成员更新，防止委员会固定成员受到贿赂攻击。具体的委员会成员选举过程和信誉管理过程分别如算法 4、算法 5 所示。

#### 算法 4 SCE/CCE 过程

该算法用于委员会成员定期更新，由旧委员会成员调用以构建新的委员会。候选人数量为  $M$ ，信誉值分别为  $R_1, R_2, \dots, R_M$ 。委员会规模为  $N$ ，选取的委员会成员为  $C_1, C_2, \dots, C_N$ ，它们的信誉值分别为  $R_{C_1}, R_{C_2}, \dots, R_{C_N}$ 。

首先，对  $M$  个候选人分别根据其信誉值执行随机验证函数  $r_i = \text{VRF}(R_i)$ ；然后，根据  $r_i$  值对  $M$  个候选人从大到小排序，得到  $C_1, C_2, \dots, C_N, \dots, C_M$ ，选取前  $N$  个候选人  $C_1, C_2, \dots, C_N$  作为新的委员会成员；最后，发起交易，公布新委员会成员。

委员会成员选举公开执行，候选人的信息记录在链上。因此，本链上的任何用户都可以识别每届委员会，无须旧委员会的帮助。另外，其他链上的委员会更新之后，需要借助旧委员会来获取更新的委员会信息。

#### 算法 5 RM 过程

委员会成员通过诚实地执行委员会节点功能，提高信誉值；反之，如果节点不能执行既定的规则，不诚实行为会对其信誉造成严重破坏。信誉激励函数的输入是委员会节点贡献值的时间加权和。在加权时考虑节点历史贡献，突出近期贡献。此外，采用不对称加权因子，使委员会节点因按照协议规则做出贡献缓慢积累信誉；如果不遵循协议，则会迅速降低信誉。

采用 Gompertz 函数<sup>[30]</sup>建模并维护委员会成员信誉  $R_{i,t} = \alpha e^{\beta e^{\gamma \sum_{\text{time}=[1,t]} \lambda^{t-\tau_0} r_{\tau,t}}}$ 。其中  $\alpha$ 、 $\beta$  和  $\gamma$  是信誉函数参数。参数  $\alpha$  决定了信誉值上限；参数  $\beta$  控制信誉函数沿  $x$  轴（节点贡献）的位移；参数  $\gamma$  调整信誉函数的增长率。本文取  $\alpha=1$ ，即信誉值的最大值  $R_{\text{Max}}$  和最小值  $R_{\text{Min}}$  分别为 1 和 0，信誉值范围为  $[0,1]$ ，其中，求和用于对节点历史贡献信息的聚合。考虑节点近期行为比过去行为更重要，引入  $\lambda$  作为历史贡献老化权重<sup>[31]</sup>， $0 < \lambda \leq 1$ ，指数项  $\lambda^{t-\tau_0}$  用于降低历史贡献的影响。 $r_{i,t}$  表示节点  $C_i$  在委员会有效期  $t$  内的贡献值，由在委员会

有效期内成功执行证明和验证的次数  $\text{succ}_i$  及不能成功执行的次数  $\text{fail}_i$  共同决定，

$$r_{i,t} = (\text{succ}_i - \text{fail}_i) / \sum_{i=[1,N]} (\text{succ}_i - \text{fail}_i)。$$

## 5 安全性分析

本节首先分析基于多委员会的跨链安全性，包括委员会可靠性、隐私保护和消息发送可靠性；然后在此基础上，对跨链交易中较复杂的跨链原子交换的原子性和终止性进行分析证明，省略对跨链转账事务的分析；最后对跨链监管的正确性、完整性和终止性进行分析证明。

### 5.1 基于多委员会的跨链安全性

#### (1) 委员会可靠性

一旦跨链请求记录在源区块链上，则该请求由该链的跨链委员会处理并通过 IID 组件传递给目标区块链跨链委员会。同样，证据信息也通过跨链委员会进行传递验证。假设在一个跨链委员会内部存在节点故障或恶意节点，在节点轮循时间内没有根据协议规定完成相应功能的节点，其行为会被 RM 组件记录，并立即由下一个轮循节点执行相应功能。理论上，只要委员会成员中存在一个诚实节点，委员会跨链功能就能正常运行。因此，跨链委员会具备可靠性。

#### (2) 隐私保护

业务链跨链通信和监管链对业务链的跨链监管都需要满足隐私保护属性，防止链内敏感信息的泄露。采用源区块链委员会和目标区块链委员会分离的方式，防止委员会权力集中，同时获取源区块链和目标区块链信息。而且，区块链委员会成员运行所属区块链上的轻客户端程序，必要时从完整节点处请求完整区块信息。另外，源区块链委员会在对区块链信息处理产生证明的过程中，采用零知识证明，在不泄露区块链隐私数据的条件下，向目标区块链证明交易的发生、事件的完成等情况。

#### (3) 消息发送可靠性

源区块链上提交的跨链请求总是可以到达目标区块链；同样，目标区块链的相应信息也可以到达源区块链。假设 Cmte\_A 想通过 IID 组件向 Cmte\_B 发送一个跨链事务（跨链交易或跨链监

管), 则即使 Cmte\_A 中只有一个诚实的节点, 也能够成功发送正确的跨链事务。假设在 Cmte\_A 和 Cmte\_B 之间存在一个经过验证的链下通信信道, 则只要有一个诚实的节点正确发送跨链消息, 消息就会到达 Cmte\_B, 并由委员会中的诚实节点接收处理。委员会成员轮循机制和基于信誉的成员激励机制, 同时保证了消息发送的可靠性。

## 5.2 业务链跨链安全性

对跨链原子交换, A 的资产在链 Pch1 上减少了  $b$ , 而在链 Pch2 上增加了  $a$ ; B 的资产在链 Pch2 上减少了  $a$ , 在链 Pch1 上增加了  $b$ , 其中链 Pch1 上的  $b$  个币与 Pch2 链上的  $a$  个币的价值相同。即 A 在链 Pch1 中转移  $b$  个币给 B, 当且仅当 B 在链 Pch2 中转移  $a$  个币给 A。以上两个事件分别记作 IA、IB。原子性指 IA 和 IB 中只有一个发生的概率可以忽略不计, 即 IA 和 IB 同时发生(资产交换)或都不发生(资产退款)。终止性指如果在时间  $T_1$  发起跨链交易, 并且在时间  $T_2$  完成或退款, 则存在时间间隔  $T_L$ , 使得  $T_2 - T_1 > T_L$  的概率可以忽略不计。如果 A 发起跨链原子交换, 交易将在预定的时间内成功或失败。

**定理 1** 所提跨链交换协议满足跨链原子性, 当以下假设成立: ① 跨链通信委员会成员至少存在一个诚实节点; ② 业务链 Pch1、Pch2 满足一致性和活跃性, 是安全的。

**证明** 证明 IA 和 IB 中只有一个发生的概率是可忽略的, 即  $IA \wedge \neg IB$  和  $\neg IA \wedge IB$  发生的概率都可以忽略不计。

$IA \wedge \neg IB$ : A 在链 Pch1 上转移了  $b$  个币给 B, 但没有在 Pch2 上收到 B 的  $a$  个硬币。根据原子交换协议, 可以将以上过程分为以下子案例: Cmte\_Pch2 未收到 Cmte\_Pch1 的交易请求, 记为 IA1; Cmte\_Pch1 收到伪造的 Cmte\_Pch2 成功质押信息, 但转账给 B, 记为 IA2; Cmte\_Pch1 收到 Cmte\_Pch2 质押不成功信息, 仍转账给 B, 记为 IA3; Cmte\_Pch2 已转账给 A, 但链 Pch2 忽略交易, 记为 IA4; Cmte\_Pch1 收到伪造的 Cmte\_Pch2 成功转账信息, 但未撤回转账, 记为 IA5; Cmte\_Pch1 收到 Cmte\_Pch2 转账不成功信息, 未撤回转账, 记为 IA6。

对案例 IA1, 存在两种情况: ① 交换请求在 Cmte\_Pch1 未能发送, 与委员会 Cmte\_Pch1 至少存在一个诚实节点假设矛盾; ② Cmte\_Pch1 已发送但未到达 Cmte\_Pch2, 与消息发送可靠性矛盾。因此, IA1 发生的概率可以忽略不计。

对案例 IA2 和 IA5, 分别存在两种情况:

① Cmte\_Pch2 伪造证明信息, 且通过 Cmte\_Pch1 验证, 与委员会 Cmte\_Pch2、Cmte\_Pch1 可靠性矛盾; ② Cmte\_Pch2 伪造证明信息, 未通过 Cmte\_Pch1 验证, 但撤销转账交易被链 Pch1 忽略, 与委员会 Cmte\_Pch2 可靠性和链 Pch1 安全性假设矛盾。同样, 案例 IA4 与链 Pch2 安全性假设矛盾。

对案例 IA3 和 IA6, 分别存在两种情况:

① Cmte\_Pch1 伪造 Cmte\_Pch2 成功, 信息验证通过, 转账给 B 且不撤销转账, 与委员会 Cmte\_Pch1 可靠性矛盾; ② Cmte\_Pch1 验证 Cmte\_Pch2 不成功信息, 并撤销转账, 但撤销转账交易被链 Pch1 忽略, 与链 Pch1 安全性假设矛盾。

综上所述, 在本文安全假设下, 案例 IA1、IA2、IA3、IA4、IA5 和 IA6 都不可能发生, 且  $IA \wedge \neg IB = IA1 \vee IA2 \vee IA3 \vee IA4 \vee IA5 \vee IA6$ , 因此  $IA \wedge \neg IB$  是不可能的。

同理, 可以证明  $\neg IA \wedge IB$  不可能。

故跨链交换协议的原子性得到保证。

**定理 2** 跨链交换协议满足终止性。

**证明** 假设业务链 Pch1 在时间  $T_1$  发起一条跨链原子交换请求, 由 Cmte\_Pch1 传递给 Cmte\_Pch2; 到时间  $T_2$ , 跨链交易完成(成功或失败)。跨链交换协议满足终止性, 即证明  $T_2$  和  $T_1$  时间间隔小于预定的时间界限  $T_L$ 。

将 Cmte\_Pch1 和 Cmte\_Pch2 获取链内信息时间分别表示为  $\delta_A$  和  $\delta_B$ , 委员会生成证明和验证证明的时间分别表示为  $\delta_{\text{prove}}$  和  $\delta_{\text{verify}}$ , 链间消息传递时间表示为  $\delta_t$ 。

如果从 A 到 B 的交换事务成功, 则总时间为  $T_{\text{success}} = 2\delta_A + 4\delta_{\text{prove}} + 2\delta_t + 4\delta_{\text{verify}} + 2\delta_B$ 。对于成功交换的事务,  $T_2 - T_1 = T_{\text{success}}$  在有限范围内。

如果交换事务不成功, 分为两种情况: ① 在完成交换事务过程中,  $[T_1, T_1 + T_{\text{success}})$  的任何时间点失败, 则总耗时  $T_{\text{fail}} < T_{\text{success}}$ ; ② 交换事务最后

失败，且需要撤销之前的转账， $T_{\text{fail}} = 2\delta_A + 4\delta_{\text{prove}} + 2\delta_t + 4\delta_{\text{verify}} + 2\delta_B + \Delta_1$ 。对于交换不成功的事务， $T_2 - T_1 = T_{\text{fail}}$  在有限范围内。

取  $T_L = \max\{T_{\text{success}}, T_{\text{fail}}\}$ ，无论跨链事务是否成功， $T_2 - T_1 > T_L$  的概率都可以忽略不计。

故跨链原子交换的终止性得到满足。

### 5.3 跨链监管的安全性

对业务链的监管包括两方面：一是业务链本身的安全性，监管链在不获取业务链原始数据的情况下验证业务链运行的正确性；二是业务链跨链交易的安全性，针对跨链转账和原子交换，发起链和接收链分别证明自己行为的完整性，进而验证跨链交易的安全性。

**定理 3** 跨链监管协议同时满足正确性和完整性，当以下假设成立：① 跨链监管委员会成员至少存在一个诚实节点；② 业务链是安全的，即满足一致性和活跃性；③ 轻客户端程序安全；④ 零知识证明安全。

**证明** 为了验证传递到监管链的  $\text{header}_{\text{pch}}$  与业务链账本一致，首先需要将  $\text{header}_{\text{pch}}$  转换为区块列表。定义算法  $\text{Longest} : \text{header}_{\text{pch}} \rightarrow \text{List}$ ，对给定  $\text{header}_{\text{pch}}$ ，输出一个代表区块链的列表  $\text{List}$ 。根据假设①、假设②和假设③，系统中会有一个诚实的委员会节点运行轻节点，并从业务链完整节点处获取区块信息，这将与业务链保持一致。根据假设④，零知识证明系统是健全的，监管链委员会成员将正确验证业务链轻客户端状态。因此，监管链确认与业务链保持一致，即业务链运行正确性得以验证。

针对跨链交易的完整性，根据上述正确性证明， $\text{Prf}_{\text{sp}}$  的正确性得到保证，监管链根据跨链交易类型分别验证  $\text{Prf}_{\text{sp}}$  中包含的跨链交易证明  $\{p_{\text{tr}}^1, p_{\text{tr}}^2\} / \{p_{\text{tr}}^1\}$ 、 $\{p_{\text{tr}}^1\} / \{p_{\text{tr}}^2\}$ 、 $\{p_{\text{tr}}^1, p_{\text{tr}}^2\} / \{p_{\text{tr}}^1\}$ 、 $\{p_{\text{tr}}^1, p_{\text{tr}}^2\} / \{p_{\text{tr}}^2\}$ ，跨链交易完整性得以验证。

**定理 4** 跨链监管协议满足终止性。

**证明** 假设监管链在时间  $T_{S1}$  发起一笔监管交易，并由监管链委员会传递给业务链监管委员会；到时间  $T_{S2}$ ，本次监管结束（监管链委员会成功提交/未提交正确监管结果）。跨链监管协议满足终止性，即证明  $T_{S2}$  和  $T_{S1}$  时间间隔小于预定的

时间界限  $T_{SL}$ 。

将委员会  $\text{Cmte\_S}$  和  $\text{Cmte\_SP}$  获取链内消息时间分别表示为  $\delta_s$  和  $\delta_p$ ，委员会证明时间和验证时间分别表示为  $\delta_{\text{pprove}}$  和  $\delta_{\text{sverify}}$ ，链间消息传递时间表示为  $\delta_t$ 。

如果监管事务成功（业务链返回证明正确信息），则总时间为  $\text{TS}_{\text{success}} = \delta_s + \delta_{\text{sverify}} + 2\delta_t + \delta_{\text{pprove}} + \delta_p$ 。当监管链验证通过业务链的证明信息后，认为此次监管是成功的。对于成功的监管事务， $T_{S2} - T_{S1} = T_{\text{success}}$  在有限范围内。

如果监管事务不成功，则存在两种情况：

① 业务链未在规定时间内  $\Delta$  内返回相应证明信息，总时间为  $\text{TS}_{\text{fail}} = \delta_s + \delta_t + \Delta$ ；② 业务链返回证明信息，但未通过验证， $\text{TS}_{\text{fail}} = \delta_s + \delta_{\text{sverify}} + 2\delta_t + \delta_{\text{pprove}} + \delta_p$ 。对于监管不成功的事务， $T_{S2} - T_{S1} = T_{\text{fail}}$  在有限范围内。

令  $T_{SL} = \max\{\text{TS}_{\text{success}}, \text{TS}_{\text{fail}}\}$ ，无论跨链监管事务是否成功， $T_{S2} - T_{S1} > T_{SL}$  的概率都可以忽略不计。

如果监管结果经过分析，需要对业务链进行进一步监管，则监管链发起一笔新的监管交易，属于两次不同监管事务。

## 6 性能评估

本节通过实验部署测试所提方案的性能，基于 Fabric 实例化了监管链和业务链，分别部署在 AMD Ryzen 7 5800H 16 GB、Intel i512500H 16 GB 和 Intel i512500H 8 GB 服务器上，每条链设置 2 个组织和 3 个共识节点。所有机器运行 Ubuntu 22.04 LTS 操作系统。不同区块链网络通过代理委员会节点连接，每个跨链委员会有 3 名成员。本文方案与文献[19-20,28]同属于基于委员会的跨链方法，但因为跨链内容处理和具体实现平台不同，数据结果没有直接可比性。本文首先测试委员会节点上传和获取不同大小数据包的速率；然后测试跨链监管时延。

### 6.1 跨链吞吐率

本节对委员会节点上传和获取区块链数据包进行测试，测试传递包的大小分别为 1 kB 和 4 kB。不同发送速率下的上传速率和获取速率如图 6 所示。对于获取操作，委员会节点从源区块链上请求获取相应数据，是查询过程，不需要经过区块

链共识, 所以访问过程更快速, 吞吐率更高, 而且获取速率受数据包大小的影响不大。随着发送速率的增加, 获取速率基本呈线性趋势。当发送速率超过 300 TPS (transaction per second) 时, 获取请求相应有所下降, 但并未达到获取请求操作阈值。对上传操作, 上传速率受数据包大小影响较大, 且随着发送速率的提高, 影响更加明显。当上传速率大于 80 TPS 时, 委员会节点上传的数据包处理减慢; 当速率超过 120 TPS 后, 上传处理性能趋于饱和, 吞吐率无法继续增长, 即上传的数据包不能立即得到执行。从上述结果看出, 在正常情况下, 即非恶意频繁跨链监管或交易, 监管链与业务链、业务链与业务链之间通过两方跨链委员会实现链接, 可以有效实现跨链监管和跨链交易, 且不会影响源区块链的运行效率。所提方案在跨链监管和跨链交易方面具有可行性。

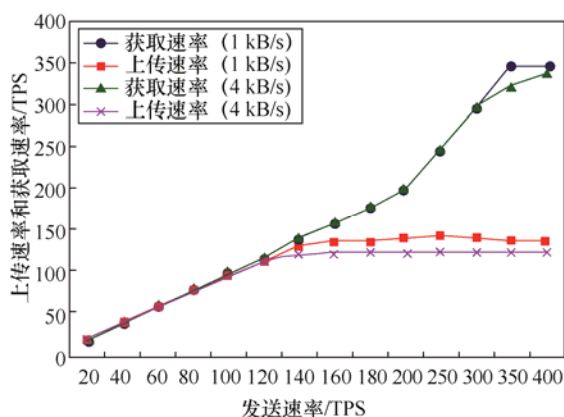


图6 不同发送速率下的上传速率和获取速率  
Figure 6 Upload rate and acquisition rate of different sending rates

## 6.2 监管时延

本节测试从监管链发起监管到确认监管结果的时延。图7是跨链监管时延分解, 包括: 监管链发起监管交易, 交易被添加到区块列表; 监管链委员会节点获取监管交易信息, 发送监管请求给业务链监管委员会; 业务链监管委员会根据监管要求获取相应数据, 并处理产生相应证明发送给监管链委员会; 监管链委员会对业务链监管委员会发来的信息进行验证, 并把监管结果上链。区块间隔和委员会查询间隔对监管时延的影响如图8所示, 其中监管时延对委员会查询间隔的敏感性较低, 因为当监管请求发生时, 委员会之间会进行主动通信。

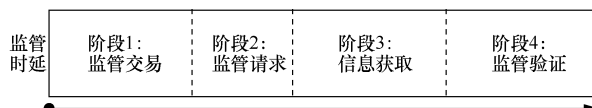


图7 跨链监管时延分解  
Figure 7 Cross-chain supervision latency decomposition

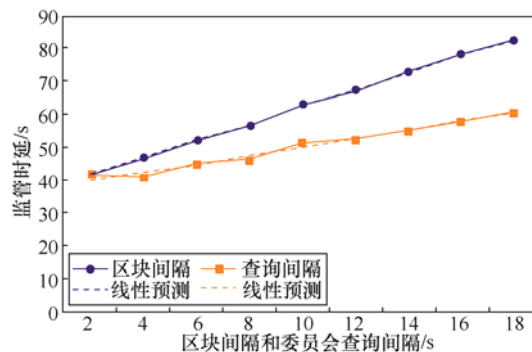


图8 区块间隔和委员会查询间隔对监管时延的影响  
Figure 8 Supervision latency of different block interval and query interval

区块间隔从两个方面对监管时延产生影响。首先, 区块间隔直接影响阶段1和阶段4的时延。其次, 区块间隔越大, 一个块中包含的监管交易数量越多。监管链委员会成员一次获得的监管需求增多, 增加了业务链监管委员会成员从业务链完整节点获取信息、验证信息并产生证明的时延。阶段2的平均时延最少, 其中包括监管链委员会成员观察间隔及链下传递监管需求。阶段3和阶段4时延最长, 因为业务链和监管链监管委员会需要分别执行隐私保护的证明和验证操作。阶段3平均时延为 18.3 s。该时延进一步划分为排队时延和业务链跨链委员会的处理时延。排队时延指业务链监管委员会节点从业务链全节点处获取相应信息的时延, 约为 0.2 s。获取相应信息后, 委员会节点对区块信息进行验证, 并基于零知识证明产生相应证明信息。最后业务链监管委员会把证明信息传递给监管链委员会。当区块间隔为 2 s 时, 阶段4平均时延为 20.87 s, 包括监管链委员会收到证明信息后对其进行验证, 以及验证完成后发布交易把验证结果提交到监管链, 经过监管链共识添加到区块。

本文跨链监管时延主要在于委员会产生和验证隐私保护的证明, 故相对于文献[19]和文献[28]的跨链时延略高。但采用分布式证明和验证方法<sup>[10]</sup>可进一步降低时延。另外, 相比文献[20]的总跨链时延, 本文具有明显优势。综上吞吐率和监管

时延分析, 本文方案具备可行性。

## 7 结束语

针对隐私保护的区块链交易系统监管难题, 本文提出了基于混合链结构的监管方案, 采用非对称委员会设计和零知识证明, 实现了通用跨链协作监管。不同于其他委员会跨链方案, 本文方案无须信任假设, 保证跨链通信和跨链监管的安全性, 证明了跨链监管和跨链交易的安全性。实验评估结果表明, 所提方案以较低的成本实现了跨链监管, 并具有一定的通用性和可扩展性。

下一步工作将重点研究以下两个方面: ① 跨链监管的安全性和执行效率, 在保证安全监管的同时提高监管效率; ② 针对多链交易系统中用户合谋问题的有效监管方法, 防止合谋对系统产生的影响, 使混合链监管框架得到更广泛应用。

## 参考文献:

- [1] ZHENG Z, XIE S, DAI H, et al. An overview of blockchain technology: Architecture, consensus, and future trends[C]//Proceedings of 2017 IEEE International Congress on Big Data (BigData Congress). 2017: 557-564.
- [2] HAYES A. Blockchain explained[EB].
- [3] NIJEHOLT H, OUDEJANS J, ERKIN Z. Decreg: a framework for preventing double-financing using blockchain technology[C]//Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. 2017: 29-34.
- [4] DAI J, VASARHELYI A. Toward blockchain-based accounting and assurance[J]. Journal of Information Systems, 2017, 31(3): 5-21.
- [5] AKINS W, CHAPMAN L, GORDON M. A whole new world: income tax considerations of the Bitcoin economy[J]. Pittsburgh Tax Review, 2014, 12(1): 24-56.
- [6] JIA X, WANG L, CHENG K, et al. A blockchain-based privacy-preserving and collusion-resistant scheme(PPCR) for double auctions[J]. Digital Communications and Networks, 2023, 5(2).
- [7] YU K, TAN L, ALOQAILY M, et al. Blockchain-enhanced data sharing with traceable and direct revocation in IIoT[J]. IEEE Transactions on Industrial Informatics, 2021, 17(11): 7669-7678.
- [8] ZHU Q, KOUHIZADEH M. Blockchain technology, supply chain information, and strategic product deletion management[J]. IEEE Engineering Management Review, 2019, 47(1): 36-44.
- [9] REN K, HO N M, LOGHIN D, et al. Interoperability in blockchain: a survey[J]. IEEE Transactions on Knowledge and Data Engineering, 2023, 35(12): 12750-12769.
- [10] XIE T, ZHANG J, CHENG Z, et al. Zkbridge: Trustless cross-chain bridges made practical[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022: 3003-3017.
- [11] 经普杰, 王良民, 董学文, 等. 分层跨链结构: 一种面向区块链系统监管的可行架构[J]. 通信学报, 2023, 44(3): 93-104.
- [12] JING P J, WANG L M, DONG X W, et al. CHA: Cross-chain based hierarchical architecture for practicable blockchain regulatory[J]. Journal on Communications, 2023, 44(3): 93-104.
- [12] BIRYUKOV A, KHOVRATOVICH D, PUSTOGAROV I. Deanonymisation of clients in bitcoin P2P network[C]//Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014: 15-29.
- [13] BIRYUKOV A, TIKHOMIROV S. Deanonymization and linkability of cryptocurrency transactions based on network analysis[C]//Proceedings of 2019 IEEE European Symposium on Security and Privacy (EuroS&P). 2019: 172-184.
- [14] GAO Y, SHI J, WANG X, et al. Practical deanonymization attack in Ethereum based on P2P network analysis[C]//Proceedings of 2021 IEEE International Congress on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking(ISPA/BDCLOUD/SocialCom/SustainCom). 2021: 1402-1409.
- [15] 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.
- [15] 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.
- [16] BELCHIOR R, VASCONCELOS A, GUERREIRO S, et al. A survey on blockchain interoperability: past, present, and future trends[J]. ACM Computing Surveys (CSUR), 2021, 54(8): 1-41.
- [17] BUTERIN V. Chain interoperability[J]. R3 Research Paper, 2016.
- [18] 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.
- [19] SHAO S, CHEN F, XIAO X, et al. IBE-BCIoT: an IBE based cross-chain communication mechanism of blockchain in IIoT[J]. World Wide Web, 2021, 24(5): 1665-1690.
- [20] ZHANG Y, GE Z, LONG Y, et al. UCC: universal and committee-based cross-chain framework[C]//Proceedings of International Conference on Information Security Practice and Experience. 2022: 93-111.
- [21] XIONG A, LIU G, ZHU Q, et al. A notary group-based cross-chain mechanism[J]. Digital Communications and Networks, 2022, 8(6): 1059-1067.
- [22] 邹萍, 李艳东, 王肖, 等. 区块链监管的现状与展望[J]. 网络安全, 2019, 10(6): 51-56.

- ZOU P, LI Y, WANG X, et al. The status quo and future trends of blockchain regulation[J]. Cyberspace Security, 2019, 10(6): 51-56.
- [23] WANG Y, GOU G, LIU C, et al. Survey of security supervision on blockchain from the perspective of technology[J]. Journal of Information Security and Applications, 2021, 60: 1-31.
- [24] 余春堂, 韩志耕, 李致远, 等. 基于区块链的众包物流分级多层智能服务交易监管架构[J]. 网络与信息安全学报, 2020, 6(3): 50-58.
- YU C T, HAN Z G, LI Z Y, et al. Blockchain-based hierarchical and multi-level smart service transaction supervision framework for crowdsourcing logistics[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 50-58.
- [25] TAO Q, CUI X, HUANG X, et al. Food safety supervision system based on hierarchical multi-domain blockchain network[J]. IEEE Access, 2019, 7: 51817-51826.
- [26] LI X, WU L, ZHAO R, et al. Two-layer adaptive blockchain-based supervision model for off-site modular housing production[J]. Computers in Industry, 2021, 128: 103437.
- [27] PENG X, ZHANG X, WANG X, et al. A refined supervision model of rice supply chain based on multi-blockchain[J]. Foods, 2022, 11(18): 1-25.
- [28] WANG K, ZHANG Z, KIM H. ReviewChain: smart contract based review system with multi-blockchain gateway[C]//Proceedings of 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCoM) and IEEE Smart Data (SmartData). 2018: 1521-1526.
- [29] PARNO B, HOWELL J, GENTRY C, et al. Pinocchio: nearly practical verifiable computation[J]. Communications of the ACM, 2016, 59(2): 103-112.
- [30] HUANG K, KANHERE S, HU W. Are you contributing trustworthy data? The case for a reputation system in participatory sensing[C]//Proceedings of the 13th ACM International Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems. 2010: 14-22.
- [31] GANERIWAL S, BALZANO L, SRIVASTAVA M. Reputation-based framework for high integrity sensor networks[J]. ACM Transactions on Sensor Networks (TOSN), 2008, 4(3): 1-37.

## [作者简介]



贾雪丹（1988- ），女，山东德州人，江苏大学博士生，主要研究方向为区块链安全、隐私保护技术。



黄龙霞（1991- ），女，江苏泰州人，博士，江苏大学副教授，主要研究方向为信息安全、云存储安全、区块链安全。



经普杰（1996- ），男，河北廊坊人，江苏大学博士生，主要研究方向为密码学、区块链安全、区块链跨链技术。



王良民（1977- ），男，安徽潜山人，博士，东南大学教授、博士生导师，主要研究方向为密码学与安全协议、物联网安全、大数据安全及区块链技术。



宋香梅（1979- ），女，吉林桦甸人，博士，江苏大学副教授，主要研究方向为信息安全和隐私保护。