重庆邮电大学研究生综述报告

|  |  |
| --- | --- |
| **报告题目** | 区块链跨链技术中的公证人机制综述 |
| **学 号** | S221231032 |
| **姓 名** | 李江权 |
| **学位层次** | 硕士研究生 |
| **学位类别** | 工学硕士 |
| **学科专业** | 软件工程 |
| **研究方向** | 区块链跨链 |
| **研究生导师师** | 曹岭 副教授 |
| **报告日期** | 2023年9月10日 |
| **报告分数** |  |
| **导师签名** |  |
| **学院审核** |  |

目录

[区块链跨链技术中的公证人机制 4](#_Toc146792625)

[1.引言 5](#_Toc146792626)

[2.公证人机制 7](#_Toc146792627)

[2.1.公证人机制的原理 7](#_Toc146792628)

[2.2.公证人机制分类 8](#_Toc146792629)

[2.2.2.单签名公证人机制 8](#_Toc146792630)

[2.2.3.多重签名公证人机制 9](#_Toc146792631)

[2.2.3.分布式签名公证人机制 9](#_Toc146792632)

[2.3不同公证人机制对比分析 10](#_Toc146792633)

[3.现有的公证人跨链方案分析 11](#_Toc146792634)

[3.1.评估标准 11](#_Toc146792635)

[3.2.公证人的跨链方案回顾 12](#_Toc146792636)

[3.2.1.改进的公证人机制 12](#_Toc146792637)

[3.2.2.公证人+HTLC 17](#_Toc146792638)

[3.2.3.公证人+侧链/中继 20](#_Toc146792639)

[3.3. 公证人跨链方案对比和分析 23](#_Toc146792640)

[4.现存问题与挑战 25](#_Toc146792641)

[5.后续工作 26](#_Toc146792642)

[参考文献 27](#_Toc146792643)

区块链跨链技术中的公证人机制

李江权

重庆邮电大学（软件工程学院）重庆 400065

联系电话: 18707095691

**摘要：**本文对区块链跨链技术中的公证人机制进行了综述，介绍了公证人机制的原理和分类，全方位地回顾了现有文献中与公证人机制相关的跨链方案，并根据去中心化程度、安全性、隐私性、可扩展性、效率和实现难度等标准进行了对比分析。本文还总结了公证人机制存在的一些问题和挑战，如信任问题、安全问题、隐私问题、可扩展性问题和实现难度问题，并提出了一些可能的改进方向。本文旨在为区块链跨链技术的研究和发展提供参考和启示。

**关键词：**区块链；区块链互操作性；公证人机制；跨链方案

# 1.引言

区块链(blockchain)是一种基于密码学原理构建的去中心化(decentralized)、无需信任(trustless)的分布式数据账本(ledger)，它记录了网络中所有节点之间发生的交易(transaction)或事件(event)，并通过共识(consensus)机制保证了数据的一致性和完整性。区块链系统不依赖于任何单一节点或机构的控制，从而具有不可伪造、不可篡改、可追溯等特点。区块链技术最早由神秘人物中本聪(Satoshi Nakamoto)于2008年提出，并作为比特币(Bitcoin,简称 BTC)[1]这种加密货币(cryptocurrency)的底层技术而出现。比特币是一种基于区块链技术实现的去中心化数字货币，它可以使网络上的多个不可信参与者之间无需可信的中央机构或第三方就能进行可信交易。自比特币问世以来，区块链技术已经取得了长足的进步，衍生出了许多新型区块链系统，如以太坊(Ethereum)[2]、超级账本(Hyperledger)[3]等。此外，区块链技术还在云计算、供应链、物联网 (IoT)、金融、电子政务、数字身份、版权保护等多个领域得到广泛应用[4-6]。

然而，区块链技术也面临着一些挑战和问题。由于区块链系统是基于密码学和共识机制构建的，每个区块链系统都有自己的数据格式、交易规则和安全策略，这使得区块链系统天然地独立于其他系统，难以与其他区块链系统或传统系统进行有效的沟通和协作，从而形成了数据孤岛(data silo)[7]。这在一定程度上违背了区块链去中心化互联的初衷，也限制了区块链技术的发展潜力。随着区块链技术的不断创新和应用，各种公有链(public chain)、私有链(private chain)、联盟链(consortium chain)等不同类型和特性的区块链系统纷纷出现，也带来了一个问题，即不同区块链系统之间如何进行通信乃至价值交换。为此，研究人员提出了跨链技术的概念，旨在通过研究跨链技术来打破不同区块链项目之间的数据孤岛，实现链间的互操作(interoperability)，解决区块链在可扩展性(scalability)、兼容性(compatibility)等方面存在的问题[8]。

跨链技术是指在不同区块链之间建立连接通道，并通过协议或机制来实现跨链交易或合约。其目标是实现真正价值的区块链网络，即能够连接同构或异构的区块链网络，并实现数据、资产和功能的跨域转移和共享。跨链技术可以根据其实现方式和特点分为以下五种主流类型：公证人机制(notary scheme)[9]、哈希锁定(hash-locking)[10]、侧链(sidechain)/中继(relay)[11-12]和分布式私钥控制(distributed private key control)[13]。这些技术在不同程度上解决了跨链互操作问题，为实现跨链提供了技术方案。哈希锁定是指通过使用密码学中的哈希函数(hash function)和时间锁定(time-locking)技术，来保证跨链交易的原子性(atomicity)和安全性。侧链/中继是一种可扩展的跨链技术，可以自行验证交易数据。侧链和中继之间没有严格的区别。从形式化的角度来看，侧链侧重于表达链之间的主从关系，而中继则是实现跨链的一种技术或解决方案。分布式私钥控制是指一种通过分布式密钥生成(distributed key generation)和门限签名(threshold signature)技术来实现跨链资产管理和转移的方式，它可以实现不同区块链之间的资产所有权和控制权的共享和转让。而公证人机制则是通过引入第三方节点或机构作为公证人来验证和确认跨链交易的有效性、合法性以及正确性，而无需对交易的细节进行验证。其优点是实现原理简单且无需复杂的工作量证明；公证人机制能够灵活地支持各种不同结构的区块链，只要公证人能够访问相关方的链上信息，就可以实现跨链交易。缺点是需要信任的公证人，可能存在中心化风险或作恶可能。

本文旨在对现有的公证人跨链方案进行多方回顾，对区块链跨链技术中的公证人机制做一次全面的总结，从而了解该技术目前存在的一些问题与缺陷，为未来的研究指明方向。主要包括以下几个方面：首先，介绍公证人跨链机制的原理；其次，对公证人技术进行分类，并分析各类公证人技术的优缺点；然后，回顾和分析现有的公证人跨链方案，并根据一定的评估标准进行对比分析；接着，总结现存的问题与挑战；最后，得出本文的结论，指明研究方向。

# 2.公证人机制

## 2.1.公证人机制的原理

如图1所示，公证人机制的工作原理是引入受信任的第三方节点或机构充当区块链之间进行跨链作互操作的公证人，这类受到信任的第三方作为双方的连接者，在跨链流程中负责跨链消息的验证和转发。

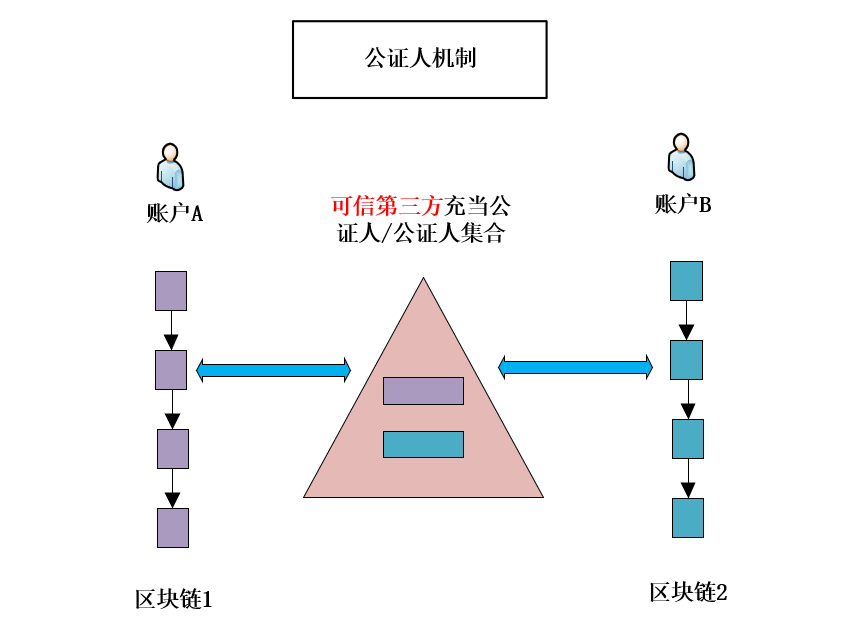


图1 公证人机制原理图

公证人机制的大致工作流程如下：

1.公证人节点需要在不同的区块链上注册并抵押一定数量的代币，以表明他们的诚信和能力。

2.当一个区块链上的用户想要向另一个区块链上的用户发送交易时，他需要先在源区块链上发起一个跨链请求，并指定目标区块链和接收地址。

3.公证人节点会监听源区块链上的跨链请求，并根据一定的规则和算法选择一部分公证人节点组成一个公证人委员会，负责处理该跨链请求。

4.公证人委员会会对源区块链上的跨链请求进行验证，确认其合法性和有效性。如果验证通过，公证人委员会会在目标区块链上发起一个对应的跨链交易，并用他们的签名来证明其真实性。

5.目标区块链上的节点会检查公证人委员会发起的跨链交易，并根据一定的共识机制来确认其是否被接受。如果被接受，目标区块链上的用户就会收到源区块链上用户发送的交易。

6.公证人委员会会将目标区块链上的跨链交易结果反馈给源区块链，并从源区块链上解锁和销毁相应数量的代币，完成跨链交易。

7.公证人节点会根据他们在跨链交易中的贡献和表现，获得一定比例的手续费作为奖励，或者因为违规或失误而受到惩罚。

## 2.2.公证人机制分类

目前，公证人机制根据实现过程中签名方式的不同，主要分为单签名公证人机制、多重签名公证人机制以及分布式签名公证人机制

### 2.2.2.单签名公证人机制

单签名公证人机制也叫中心化公证人机制，通常由单一指定的独立节点或者机构充当，它同时承担了数据收集、交易确认、验证的任务。公证人在该交易过程中充当交易确认者和冲突仲裁者的角色，是用中心化机构替代了技术上的信用保障，这种模式虽然交易处理速度快，兼容性强，技术架构简单，但中心节点的安全性也成为系统稳定的关键瓶颈。最传统的公证人机制就是基于中心化交易所得跨链资产交换，这种跨链的方式比较单一，只支持资产的交换。基于单签名公证人机制的以太坊网络与比特币网络之间的资产交换流程如图2所示。

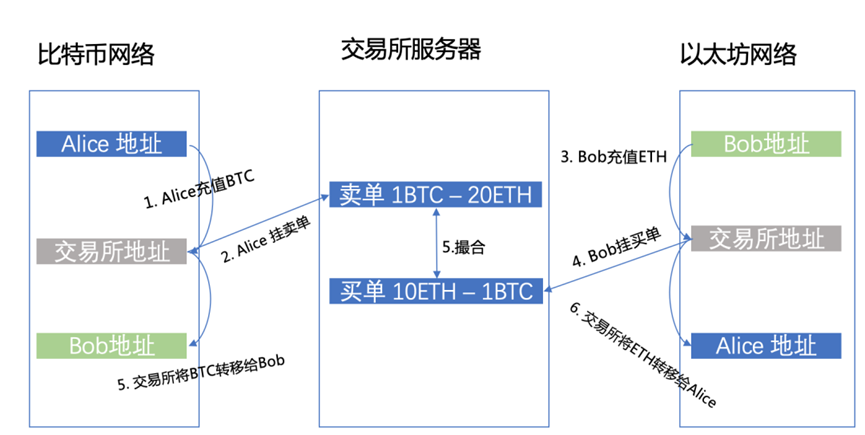


图2单签名公证人之间的跨链资产交换流程图

### 2.2.3.多重签名公证人机制

多重签名公证人机制中公证人是一群机构组成的联盟，跨链资金的转移由这个联盟所控制的。在这种机制中，每个公证人节点都有一个密钥，它们需要在各自的账本上对跨链交易进行签名。只有当签名的数量或比例达到一定的要求时，跨链交易才能被确认。这种方式比单签名模式更安全，因为即使有少数的公证人被攻击或者作恶，也不会影响系统的正常运行。多重签公证人机制示意图如图3所示。

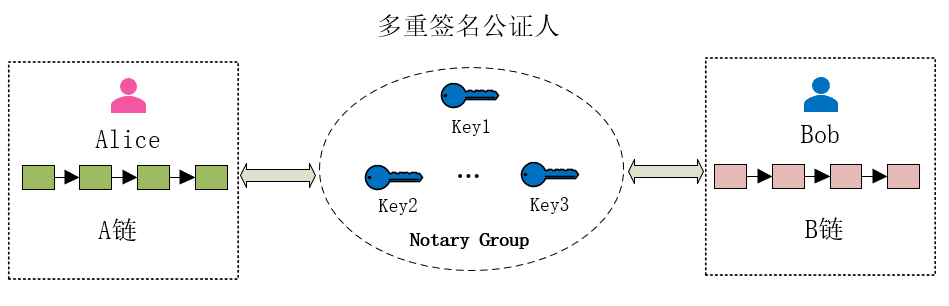


图3 多重签公证人机制示意图

### 2.2.3.分布式签名公证人机制

分布式签名公证人机制[13-14]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机制。与多重签名公证人机制相比，分布式签名公证人机制采用MPC（多方计算）[15]的核心思想来保证密钥的安全性和隐私性[16][17]。分布式签名公证人机制的实现过程是将基于密码学生成的唯一密钥分割成多个片段，并将处理后的片段随机分发给选定的公证人。即使所有公证人将碎片拼凑起来，也无法获得密钥。只有允许一定比例的公证人共同完成签名，才能拼凑出完整的密钥，从而实现更加去中心化的跨链交互。分布式签名公证人机制示意图如图4所示。

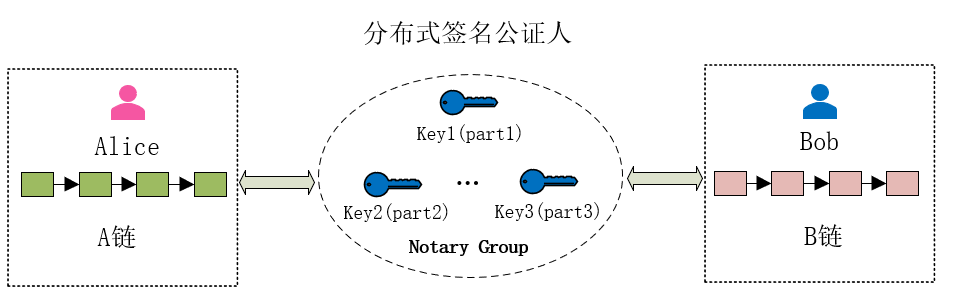


图4 分布式签公证人机制示意图

## 2.3不同公证人机制对比分析

三种不同类型的公证人机制在实现过程中采用了不同的数字签名技术，这就导致了它们在去中心化程度、安全性、效率、兼容性、实现难度等方面存在很大的差异，而这些差异产生的根本原因是不同公证人机制所对应的数字签名技术的密码管理方式和密码算法不同[18-21]。表1展示了三种公证人机制在各个方面的对比分析结果。

表1 三种公证人机制各方面对比表

|  |  |  |  |
| --- | --- | --- | --- |
|  | 单签名公证人机制 | 多签名公证人机制 | 分布式签名公证人机制 |
| 密码管理方式 | 单一私钥 | 多个私钥 | 单个私钥的分布式共享 |
| 加密方案 | 公钥加密 | 公钥加密 | 公钥加密 |
| 密码算法 | 非对称加密算法 | 多重签名算法 | 多方计算算法 |
| 去中心化程度 | 最低 | 中等 | 最高 |
| 安全级别 | 最低(单点故障) | 中等(消除单点故障) | 最高(分布式计算技术) |
| 交易处理速度 | 最快 | 较慢 | 最慢 |
| 可扩展性 | 有限 | 中等 | 最高 |
| 实现难度 | 简单 | 中等 | 复杂 |

# 3.现有的公证人跨链方案分析

## 3.1.评估标准

为了对现有的公证人跨链方案进行分析，我们需要从不同的角度来评估它们的优劣。因此，在对各文献中提到的公证人跨链方案进行回顾之前，本文主要考虑以下几个评估标准：

1.去中心化程度：是指公证人跨链方案在设计和实现上是否依赖于中心化的节点或机构，参与者之间的权力分配是否均衡，以及是否存在单点故障或作恶的可能。通常，用公证人节点的数量、选择方式、激励机制、权力分配情况等指标来衡量去中心化程度。

2. 安全性：是指能够抵抗各种攻击和威胁，保证跨链交易的正确性和不可篡改性的能力。安全性越高，越能维护区块链的信誉和稳定性。通常，用公证人节点的可信度、攻击者需要控制的公证人节点比例、是否有有效的验证和共识机制、是否有足够的激励和惩罚机制、跨链交易的撤销难度等指标来衡量安全性。

3. 隐私性：是指跨链方案能够保护跨链交易参与者的身份和数据不被泄露或滥用的能力。通常，用公证人节点能否轻易访问到参与者的用户身份信息、公证人节点能否轻易查看到跨链交易的隐私、是否有合理的数据访问和共享规则、是否使用加密或匿名技术等指标来衡量隐私性。

4. 可扩展性：是指能够支持不同的区块链系统进行跨链互操作的数量，以及能够处理多大的跨链交易量和频率的能力。可扩展性高的公证人跨链方案可以连接更多的区块链系统，并且能够应对更高的跨链交易需求，从而提高跨链生态系统的规模和效率。通常，用支持的区块链系统类型和数量、每秒处理的跨链交易数、每笔跨链交易所需的资源等指标来衡量可扩展性。

5. 效率：是指能够快速地完成跨链交易，提高用户体验和满意度的能力。效率高的公证人跨链方案可以降低用户等待时间，提高系统吞吐量和响应速度。通常，用每笔跨链交易所需的时间、费用、步骤等指标来衡量效率。

6. 实现难度：是指公证人跨链方案在设计和开发上所面临的技术挑战和复杂度。实现难度越低，跨链方案越容易被实现和部署，也越容易被接受和推广。

## 3.2.公证人的跨链方案回顾

目前，相关的文献中已经提出了一系列关于公证人机制的跨链方案。根据不同的特点主要有以下三类：

1. 改进的公证人机制跨链方案
2. 公证人+**HTLC**的混合型跨链方案
3. 公证人+侧链/中继的混合型跨链方案

接下来，本文将会依次对以上三类跨链方案涉及文献进行一个回顾，以便我们根据评估标准，从不同的角度来对它们进行对比和分析。

### 3.2.1.改进的公证人机制

虽然传统的由单一指定的独立节点或者机构充当公证人的跨链方案响应速度快，兼容性强，技术架构简单，但是中心化的程度过高，很容易出现单点故障或作恶。改进的公证人机制则是指在传统的公证人机制的基础上，引入一些非混合型机制的改进措施或者设计出不同以往的公证人机制的优化方案，如增加公证人的数量和多样性，优化公证人的选举方式，采用多重签名或分布式签名技术，引入激励和惩罚机制等，以提高公证人的可信度和安全性。

Xiong等人[22]提出了一种基于公证人组的跨链交互模型，实现了不同区块链之间的价值转移，其模型如图5所示。该模型分为预交易阶段和正式交易阶段，通过引入了保证金池和声誉机制，保证了跨链交易的原子性和一致性。此外，该跨链交互模型还设计了一个基于声誉的公证人选举机制和一个激励机制，鼓励公证人群中的成员参与跨链交互，提高了公证人群的可靠性和活跃度。

MetaOpera[23]是一种跨元宇宙互操作性协议，它使用了阈值签名的公证机制，以及基于区块链技术的中继元宇宙和NFT技术。MetaOpera可以连接任何类型的元宇宙，无论是基于区块链还是基于中心化服务器的，并实现了数据、资产、身份和功能的无缝交换和共享。MetaOpera的公证人委员会是由生成连续区块的节点组成的一个动态变化的集合，他们使用了多重签名、环可验证随机函数、权益证明等技术来验证和转发跨元宇宙消息，并保护各方的隐私。MetaOpera的协议分为注册阶段、交易阶段、执行阶段和公证阶段，以实现跨元宇宙互操作的有效性和原子性。

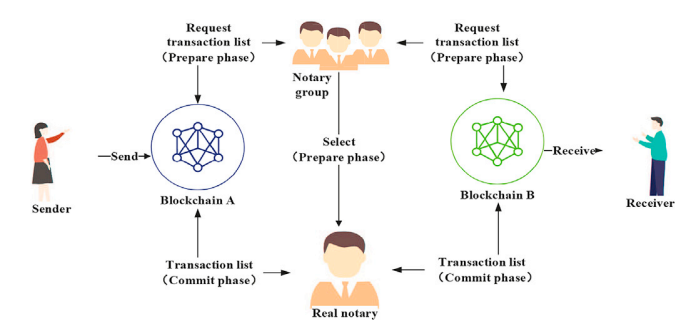


图5 基于公证人组的模型

Wang 等人[24]提出了一种基于双层能源区块链网络的可信对等能源交易模式，其中公证人机制是保证跨链信息互操作和可信度的关键技术。公证人机制通过信用评估和阈值设置，动态地选择高信用的节点组成验证节点子组（VNS），并通过区块链数字签名对子链和主链之间的信息进行验证。信用评估包括合约履行、共识参与和交易热情三个方面，以激励节点诚信地参与能源交易和区块验证。阈值设置可以减少公证人节点的数量，提高跨链通信的效率。此外，双层能源区块链网络中还设计了一个环形映射身份认证算法，给每个能源参与者一个准确、可追溯的身份实体，优化了公证人机制的安全性和可靠性。

Cao 等人[25]提出了一种基于公证人组的跨链数据溯源方法，用于解决不同信任域下的数据交易和访问问题。该方法通过建立全局的授权链和域内的访问链，实现了数据资产的全球授权和交易，以及跨域数据的访问和溯源。同时，该方法引入了基于声誉值的公证人选举模型，提高了公证人组的可信度，解决了跨域用户之间的信任问题。通过基于数据指纹的跨域数据溯源机制，该方法能够关联和追踪全球数据所有权交易、访问控制策略和用户访问记录，实现了跨域数据交易、权限授予和用户访问行为的溯源。实验结果表明，该方法能够有效地支持全球数据资产的授权和交易，以及跨域数据的访问和溯源。

Wu等人[26]在跨链数据交换中引入周期委员会的概念，提出了一种基于委员会周期性轮换机制的跨异构区块链通信通用框架，支持跨多个异构区块链系统的多种交易信息交换。作者采用多重签名公证人的方式，设立由公证人组成的周期委员会，通过周期委员会和设计协议制定规范，从而连接异构区块链，从委员会中随机挑选公证人，并给每一组委员会都设立周期时间，最终实现跨链交易。该方案比传统公证方法具有更强大的信任，相比传统的单公证人而言，由公证人组成的委员会可以有效杜绝单点故障问题，还能提升系统整体的去中心化程度；相比普通的公证人组而言，系统会随机挑选公证人进入委员会，且系统会对参与每一次跨链交易的委员会都会设立时间周期，保证参与跨链交易的公证人都是离散分布的，以此减少公证人组的串谋攻击，保证跨链交易正常执行。

Wang等人[27]提出了一种量子环境下公证系统的跨链交易模型，该交易模型中使用PageRank选举算法[28]和多签名公证人机制，通过实现资产量子冻结算法实现了源链的资产冻结和证明，然后公证人通过量子分散有序多重签名共同签署交易，实现了跨链的资产转移。在选举过程中，采取的是改进的PageRank算法的跨链公证人选举模型，该方法可以收集多种公证人节点相关信息，然后利用改进的PageRank算法对公证人节点进行重要度计算，得到高可信的公证人节点。

Tian等人[29]提出了一种基于智能合约的去中心化跨加密货币交易方案，可以让用户之间通过不同的账户进行不同类型的加密货币之间的交易。该方案中的中间人为跨链资产转移提供不同的资产类型，并在交易过程中向智能合约提供跨链交易双方的转账情况用于交易验证，以便智能合约执行下一步。在方案执行时，跨链用户会选择拥有足够跨链双方区块链资产的中间人。在交易验证时，会通过PoW算法从没有参与此次交易的中间人中选举验证者，来验证跨链区块链上转账是否成功。该方案中使用PoW算法来选举验证委员会，使得每个中介节点都需要付出一定的成本和努力才能加入验证委员会，并且每个中介节点都有相同的机会被选中。这样，可以保证验证委员会的随机性和公平性，并且可以抵抗少数恶意节点的攻击。

HARB[30]是 Karumba 等人提出的一个基于超图的自适应联盟区块链框架，能够在一定程度上解决分布式能源交易（DET）中的可扩展性、隐私和互操作性等挑战。HARB利用超图的概念来描述节点之间的高阶关系，并根据这些关系将网络划分为多个子链。HARB引入了一个分布式公证人模块，用于在不同的子链之间进行交易验证和价值转移，从而实现互操作性。该分布式公证人是从每个子链中选出的高可靠性节点，它们通过超图横断的方法保证至少有一个节点参与跨链交易的验证。引入分布式公证人模块之后，该解决方案可以有效地消除中心化数字公证人方案中存在的单点故障的风险。此外，HARB还提出了一个数据标记和匿名化模型（dTAM），用于保护交易数据和用户隐私。

Yin等人[31]提出了Bool Network，一个基于分布式签名公证人的开放、分布、安全的跨链公证平台。Bool Network实现了演进的隐藏委员会，分为注册、选举和交接三个阶段。在注册阶段，参与者需要绑定一定量的资产和公钥，以增加选举概率。在选举阶段，参与者通过Ring-VRF方案进行身份隐藏和随机性证明，以获得委员会资格。在交接阶段，委员会成员通过零知识证明的混合解密方案进行身份验证和秘钥交换。为了保护秘钥的机密性和完整性，所有密钥管理过程都在可信执行环境(TEE)中执行。Bool Network采用分布式签名公证人，以实现高度去中心化和安全性。Bool Network还采用类似原子交换的机制来保证交易原子性，但缺乏用户身份隐私的保护。

IBE-BCIOT [32]是Shao等人提出了一种基于身份识别加密（IBE）的区块链在物联网（IoT）环境中的跨链通信机制，其总体框架如图6所示。该机制通过选举每个区块链的代理节点，并将代理节点的ID作为公钥传递给跨链公证人。跨链公证人通过IBE机制计算出相应的私钥，并以安全的方式返回给代理节点，从而实现不同区块链之间的安全高效通信。该机制还提供了两种跨链通信方案：代理节点之间的直接跨链通信方案和通过公证人的间接跨链通信方案。公证人是指在跨链通信中，负责验证不同区块链之间交易的真实性和合法性的第三方节点。IBE-BCIOT中的公证人的选举方式和代理节点的选举方式一致，都是基于密度峰值的聚类算法，该算法根据每个节点的计算能力和网络传输成本来确定最优的公证人。具体步骤如下：

1.计算出每个节点的局部密度ρi，即在一定距离dc内与该节点相邻的节点数量。

2.计算每个节点与具有更高密度的任意节点之间的最小距离δi，即该节点到其密度最近邻的距离。

3.根据ρi和δi的值，选择具有较高密度和较大距离的节点作为公证人，即满足密度峰值条件的节点。

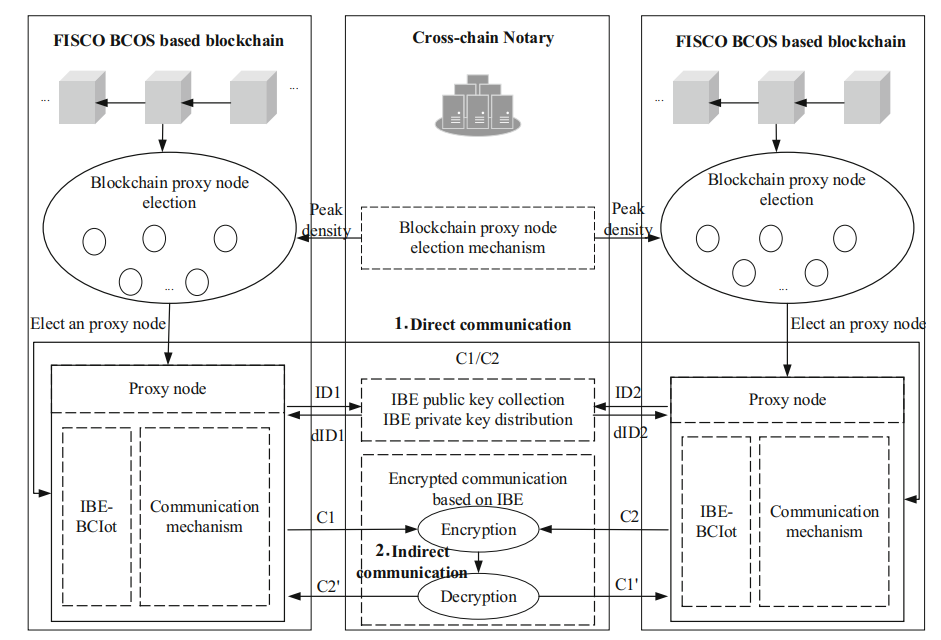


图6 IBE-BCIOT机制总体框架

CCIO[33]是Lu等人提出了一种利用公证人模式的预言机作为中介方，实现不同区块链之间的数据交互和价值流通的跨链方案，设计了一个基于区块链预言机技术的跨链架构，并提出了一种双向信息跨链交互方法。CCIO是双向信息跨链交互方法，对三种传统的区块链预言机模式进行了改进，并结合了对称和非对称密钥的混合加密方式，保证了跨链数据的安全性。此外，CCIO方案中设计了一个基于区块链预言机技术的跨链架构，包括参与跨链的联盟区块链和基于公证人模式的高效跨链预言机两个主要模块，前者是具有跨链需求的联盟区块链，后者是通过改进多种传统预言机模式构建的跨链中介方。

DeXTT协议[34]是Borkowski等人提出的一种跨链资产转移协议，它采用了多公证人竞争的机制。DeXTT协议利用claim-first transactions的模式以及deterministic witness[35]的传播和竞争，确保了不同链上资产的最终一致性。DeXTT协议采用了一种确定性见证的公证人选举方案，用于在跨区块链转账中选择一个公证人并给予奖励。该方案首先由转账双方签署一个转账意图（PoI），并在任意一个区块链上发布一个CLAIM交易并公开PoI，任何观察到CLAIM交易的参与者都可以成为见证者，通过在所有区块链上发布CONTEST交易，传播PoI，并对其进行签名。在转账有效期结束后，任意一方可以在所有区块链上发布FINALIZE交易，结束竞争，并根据转移双方签署的转移意图（PoI）的签名和见证候选人的公钥c签名的哈希差值来选举获胜者[35]。签名值最小（最接近于零）的竞争者将被选为获胜者，并获得公证人奖励。这种公证人选举方案的优点在于：1）它是纯粹的确定性的，不依赖于任何随机因素或外部输入；2）它是公平的，签名值是由转账信息和竞争者的公钥决定的；3）它是可预测的，任何区块链上都可以根据相同的算法计算出相同的获胜者。

### 3.2.2.公证人+HTLC

纯公证人方案使用受信任的第三方作为中介，为双方验证和转发跨链消息，但是公证员可能被恶意或受到损害，以及缺乏公证员履行职责的激励。哈希锁定是一种使用加密哈希来锁定和解锁不同区块链上的资产的技术，它要求双方生成并交换可以解锁哈希值的密钥，但应用场景仅限于资产交换，且容易遭受失败者攻击、虫洞攻击等攻击。因此，诞生了公证人机制结合哈希时间锁这一新颖的跨链方案，它结合了两种方法的优点来解决了它们的问题。该方案基本思想是利用公证人作为中介，引入了对公证人的奖励和惩罚，通过哈希时间锁合约（HTLC）来保证跨链交易的原子性和安全性。

Thomas等人[36]提出的Interledger就是一种典型的公证人结合哈希时间锁合约的混合跨链协议。Interledger是一种跨链支付协议，它可以在不同的区块链或支付网络之间实现安全和原子的资金转移。为了完成这一目标，它结合了公证人和哈希时间锁合约 (HTLC) 的技术，并使用了一系列的协议和数据结构。首先，它使用一种特殊的数据结构，称为Interledger Packet，来封装跨链支付的相关信息，如支付金额、目标地址、过期时间和条件等。然后，它通过一种传输层协议，称为Interledger Protocol (ILP)，来在不同的区块链或支付网络之间传输Interledger Packet。为了保证跨链支付的安全性和原子性，ILP依赖于一种中介服务，称为公证人。公证人需要与支付方和收款方建立信任关系，并承诺在条件满足时转移资金，或者在过期时间到达时退还资金。公证人之间可以使用HTLC来实现资金的转移，HTLC是一种智能合约，它可以根据条件和过期时间来控制资金的释放或退回。最后，为了寻找最优的支付路径，Interledger使用一种路由层协议，称为Interledger Quoting Protocol (ILQP)，来在不同的公证人之间进行查询。ILQP可以根据支付金额、目标地址、过期时间和条件等因素来选择最合适的公证人，并提供相应的汇率和费用信息。

Dai等人[37]在公证人和用户协商的基础上提出了一种基于改进哈希锁定的跨链交易模型。该模型涉及三种角色：用户、独立区块链和跨链系统。跨链系统充当中介，协调交易过程，并提供候选公证节点来监控每个区块链中的交易。该跨链方案中的跨链交易分为三个阶段进行，用户在需要进行跨链交易的每个独立区块链中都有自己的地址和密钥。资产锁定阶段，他们分别用跨链系统选择的公证节点提供的密钥锁定资产，防止用户在交易过程中撤回资产；密钥协商阶段，公证节点分别与用户协商用于交易解锁的密钥，该密钥基于Diffie-Hellman算法生成，保证密钥的安全性和随机性；交易处理阶段，利用协商的密钥和锁定的资产进行交易，公证节点监控和协调区块链A和B中的智能合约的执行，这样就可以保证交易的正确性和原子性。此外，该模型还设计了一个基于哈希锁定的跨链资产交换的智能合约，使得公证节点可以通过协商的密钥来协调交易。使得保证交易安全的同时，保持了执行时间和资源使用的稳定水平。

Yu等人[38]提出了一种基于区块链的跨链身份认证方案，该方案通过结合公证机制和哈希锁定技术，实现了不同区块链之间的身份认证和资产转移。该方案将跨链身份认证分为三个阶段：身份认证阶段、预交易阶段和正式交易阶段。在身份认证阶段，该方案通过信誉值排名和激励机制，选举出n个信誉值高于初始值n的节点作为公证人。在正式交易阶段，该方案利用哈希时间锁技术，要求交易双方在给定的时间内提供正确的哈希值，否则交易将失败并退还资产。在解决传统跨链技术中存在的公证人中心化、交易效率低、安全性差等问题。通过结合哈希锁定技术，该方案在一定程度上解决了传统跨链技术中存在的公证人中心化、交易效率低、安全性差等问题，并提高跨链身份认证和资产转移的可靠性和效率。

Sun等人[39]提出了一种基于公证人方案和哈希时间锁的去中心化跨链服务协议，通过选举主公证人和次公证人，以及使用哈希值作为跨链交易的参数，实现了不同区块链之间的数据和资产交换，其交易流程如图5所示。此外，该协议设置了一种激励机制，通过锁定违约金和更新信誉值，保证了公证人和参与者的诚信行为，提高了跨链交易的效率和安全性，其二级公证人的选举程序如图6所示。该协议在可扩展性、可验证性和抗审查性等方面表现良好，同时在实验上也验证了其可行性和优越性，为区块链跨链服务的研究提供了一个有价值的参考。

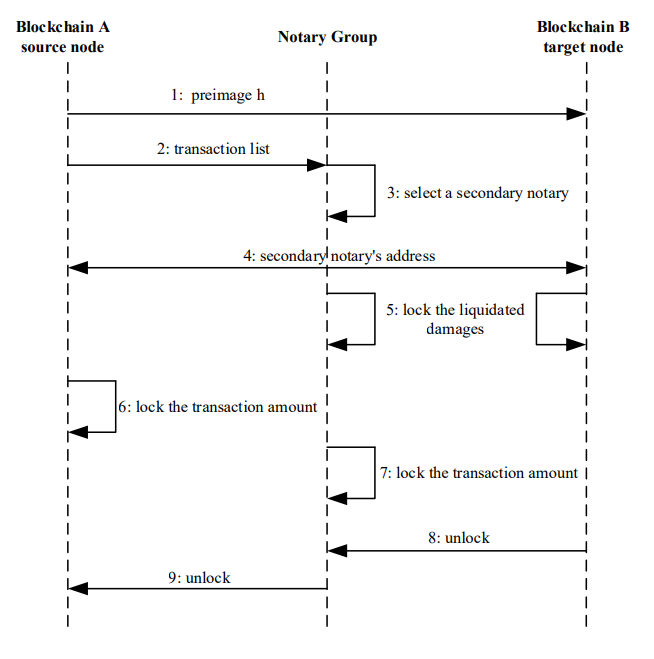


图6 交易流程

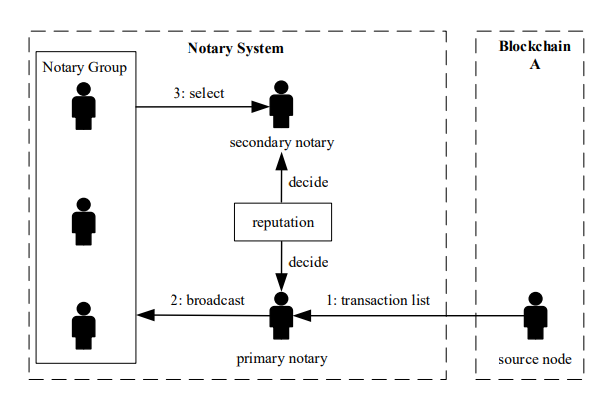


图7 二级公证人选举程序

为了实现元宇宙环境中不同区块链之间的数字内容和数字资产的跨链互动，Ren等人[40]提出了一种基于改进的哈希时间锁（HTLC）和公证人机制的跨链交易方案，称为HCNCT，其跨链系统的模型结构如图7所示。该方案主要包括交易准备阶段、正式交易阶段和交易验证阶段三个阶段。在交易准备阶段，交易发起用户与公证人组协商生成哈希锁的原像，并初始化交易；在正式交易阶段，双方用户使用相同的哈希值锁定各自的资产，并在限定时间内使用哈希锁的原像解锁资产完成交易；在交易验证阶段，双方用户对交易信息进行签名，并发送给公证人组进行验证。HCNCT方案中引入的是一种公证人组的机制，公证人组由多个公证人组成，通过密钥协商和可验证秘密分享技术，实现对整个交易过程的监督和参与，有效地解决了传统HTLC方案中存在的恶意超时交易攻击以及单一公证人机制的中心化问题。此外，HCNCT方案中设计了用户信誉评估机制和公证人组管理机制，用于减少用户恶意违约的发生，激励用户积极促成正确的交易，并保证公证人的可信度。

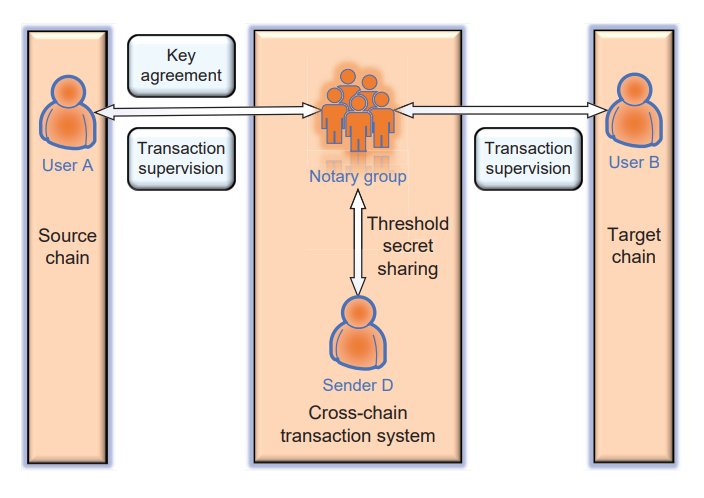


图7 HCNCT跨链系统的模型结构

### 3.2.3.公证人+侧链/中继

公证人结合侧链/中继是一种比较常见的混合机制，在这种方案中，公证人负责在两个区块链之间传输信息和验证信息真实性，还负责在跨链交易中处理资产的转移和确认。与此同时，通过实现侧链/中继，维护一条链接源链和目标区块链的中继链，通过公证人对用户资产锁定的确认和中继链，可以将源区块链的代币映射到中继链上来，实现跨链资产转移，也可以在中继链上进行代币交换，最后通过资产赎回，完成跨链资产交换。

AgentChain[41]是Dawei等人提出的一个基于多重签名的去中心化跨链资产交换系统，实现了从现有链到AgentChain的资产映射和在AgentChain上的代币交换。AgentChain是一种基于公证人+侧链的跨链交易系统，它利用交易运营商组（TOG）作为公证人，为用户提供资产映射和交换的服务。TOG由多个交易运营商（TO）组成，每个TO都需要在现有链上锁定一定数量的代币作为抵押，并创建一个多重签名的存款池。用户可以根据TOG的存款量和声誉评分选择一个合适的TOG，并向其存款池转账资产，从而在AgentChain上获得相应数量的代币。用户可以在AgentChain上进行代币的公平交换，也可以随时提取资产。如果TOG拒绝或延迟提供服务，用户可以向AgentChain上传仲裁请求和证据，要求惩罚该TOG并获得赔偿。AgentChain采用多重签名公证人机制，保证了跨链交易的安全性和原子性。AgentChain与大多数现有的区块链项目兼容，只要求它们支持多重签名。Practical AgentChain[42]是Hei等人在AgentChain的基础上进行了改进和扩展构建了的一个综合的跨链交易系统。Practical AgentChain支持各种币种到对应代币的映射和交易，引入了Town crier作为可靠的数据预言机系统，获取跨链交易的状态，并结合了一个匹配交换协议，保证了链上代币交换的公平性。此外，Practical AgentChain还设计了一个公正的服务仲裁机制和一个押金分配方案，保证了系统的可靠性。由于系统架构的高可移植性，Practical AgentChain可以部署在任何支持智能合约的现有区块链上。

Jiang等人[43]提出了一种利用公证人结合侧链的跨链方案，实现多个区块链系统的集成。公证人是一种特殊的网络服务，负责在不同的区块链系统之间进行交易验证和数据路由，以及提供时间戳和排序服务。该方案设计了两种公证人机制，一种是在联盟链中，用于在联盟成员之间达成共识和执行智能合约，另一种是在侧链中，用于将子网与主网进行合并和分离。公证人是由子网内的物联网设备随机选出的，每个设备都有一定的概率成为公证人。此外，该跨链方案还使用了预言机服务，当一个区块链需要从另一个区块链或外部世界读取数据时，通过公证人进行数据获取和验证。

AbitBridge[44]是由Pang等人基于主-子链架构提出的一种结合中继链和公证人的跨链协议技术解决方案。该方案在主-子链架构中增加了一条子链，名为TVC（交易验证链）。TVC通过利用共识机制改变了公证人方案原有的链下验证流程，增强了公证人方案的安全性。作为中继链的角色，TVC需要负责转发和验证跨链消息，与每条链上的跨链桥组件进行通信，并利用RVC（可靠验证调用）模块来调用智能合约完成跨链操作。此外，为了保证跨链交易的原子性，AbitBridge还设计了异常处理组件和回滚组件。AbitBridge方案无需对每条链进行底层改造，而是主要依赖于智能合约的跨平台特性，通过监控跨链桥组件实现跨链消息传递。

PXCrypto[45]是Zhang等人提出的一种受监管的跨链保密交易方案，它使用一个中继链和一个公证人机制来实现不同区块链平台之间的代币映射和交换。它设立了一个监管机构，负责对用户的身份进行认证和监管，以及对交易结果进行仲裁。它还使用了一个资产质押服务商，负责将其他区块链上的代币兑换成相应的包装代币，并提供给用户。用户可以在中继链上使用包装代币进行交易，而不暴露自己的真实身份和订单价格。为了保护用户的数据隐私，PXCrypto提出了一个代理多方计算（MPC）的方法，通过非对称加密和门限秘密共享，让一个由质押金额决定的委员会在不知道订单明文价格的情况下进行订单匹配。此外，PXCrypto与Hyperledger Fabric兼容，使用Idemix机制对用户进行身份管理。PXCrypto在很大程度上提高了跨链交易的安全性和公平性，但同时也牺牲了一定的去中心化程度和不可区分性[46-47]。

Vger[48]是Shu 等人提出的一种基于可验证随机函数（VRF）和门限密码学的跨链方案。Vger使用了一个中介账户作为跨链交易的桥梁，这个中介账户是一个智能合约，可以在不同的区块链网络上部署。跨链方案通过可验证随机函数（VRF）基于密码学的抽签来选择中介账户的管理委员会(即公证人组)，而该委员会则需要对跨链交易进行签名和验证。此外，Vger还利用门限密钥技术来管理中介账户，只有当超过一定比例的公证人对跨链交易达成共识时，才能解锁中介账户的资产，并通过智能合约来实现原子交换。

叶等人[49]提出了一种面向联盟链的分布式公证人跨链模型，该模型利用原有的公证人机制，将公证人设计为由各个局部链推选的节点组成的全局链，从而提高了跨链操作的去中心化程度和安全性。该模型中的跨链网络由多条局部链和一条全局链组成，局部链是各个联盟链的成员，全局链是由各个局部链推选出的公证人节点组成的一条公共链，作为跨链媒介。全局链上运行一个智能合约，用于记录和验证跨链请求和响应。局部链和全局链之间通过一个跨链中继器进行通信，跨链中继器是一个软件模块，负责转发和广播跨链消息。

Karumba 等人[50]提出了一个名为BAILIF的区块链互操作性框架，BAILIF采用三层架构，包括网络层、共识层和应用层。网络层使用超图遍历的概念来选择不同区块链网络中的节点作为公证人，从而实现去中心化的公证服务。共识层定义了跨链认证和验证（XCAV）协议，以验证和验证跨链交易，并保证交易的ACID属性。应用层提出了一个跨链工作流引擎（XCWE），使用智能合约来确保合约协议在链上进行并透明地批准。XCWE将合约协议分解为可以在区块链网络上执行的单个原子交易。应用层提供技术来将合约和业务流程编码为智能合约，以实现应用层互操作性。

## 3.3. 公证人跨链方案对比和分析

在此小节中，本文根据去中心化程度、安全性、隐私性、可扩展性、效率、实现难度等评估标准，对上述文献回顾中所提到的不同的公证人跨链方案的进行进行了对比和分析，得到的相关性能的对比分析结果如表2所示。

表2 不同公证人机制优化方案性能对比表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 方案 | 去中心化程度 | 安全性 | 隐私性 | 可扩展性 | 效率 | 实现难度 |
| 改进的公证人机制 | 中等 | 中等 | 低 | 高 | 高 | 低 |
| 公证人+HTLC的混合机制 | 高 | 高 | 中等 | 中等 | 中等 | 中高 |
| 公证人结合侧链和中继的方式 | 高 | 高 | 中高 | 高 | 中高 | 高 |

此外，我们通过分析相关文献中提及的三类不同的公证人机制优化方案，得到以下结论：

改进的公证人机制：该方案通过优化公证人的选举和设计，提高了去中心化程度和安全性，但仍然存在公证人节点可能被攻击或作恶的风险，以及公证人节点可能泄露或滥用跨链交易数据的问题。该方案具有较高的可扩展性和效率，因为它可以支持多种类型的区块链系统进行跨链互操作，并且可以快速地完成跨链交易。该方案的实现难度较低，因为它只需要对公证人机制进行一些调整优化，而不需要引入其他的技术或机制。

公证人+HTLC的混合机制：该方案通过结合哈希时间锁合约和公证人机制，提高了安全性和隐私性，因为它可以保证跨链交易的原子性和不可篡改性，防止了双花和欺诈的风险，以及保护了跨链交易参与者的身份和数据不被泄露或滥用。该方案具有较高的去中心化程度，因为它不依赖于中心化的节点或机构，而是由多个公证人节点共同参与和监督跨链交易。该方案的可扩展性和效率较低，因为它需要在不同的区块链系统之间建立哈希时间锁合约，并且需要等待公证人节点对跨链交易进行验证和确认。该方案的实现难度较高，因为它需要在不同的区块链系统之间实现哈希时间锁合约，并且需要协调公证人节点之间的行为和激励。

公证人结合侧链和中继的方式：该方案通过利用侧链和中继链作为跨链交易的载体和桥梁，提高了可扩展性和效率，因为它可以连接更多的区块链系统，并且可以为主链提供更多的功能和性能。该方案也提高了安全性和隐私性，因为它可以利用侧链和中继链上的验证和共识机制，保证跨链交易的正确性和不可篡改性，并且可以利用加密或匿名技术，保护跨链交易参与者的身份和数据不被泄露或滥用。该方案具有较高的去中心化程度，因为它不需要依赖于中心化的节点或机构，而是由多个公证人节点对跨链交易进行验证和监督。该方案的实现难度较高，因为它需要在不同的区块链系统之间建立侧链和中继链，并且需要协调公证人节点之间的行为和激励。

# 4.现存问题与挑战

公证人机制是一种常用的跨链技术，它通过引入第三方节点或机构来实现不同区块链之间的交易验证和转发。 然而，公证人机制也存在一些问题和挑战，主要包括以下几个方面：

信任问题：现有的跨链方案已经提出了一系列选举可信公证人的方式，但很多方式选出来的公证人仍有很大几率可能作恶。因此，如何选择更加可信的公证人，以及如何设计更加有效的激励和惩罚机制，是公证人机制需要解决的重要问题。

安全性：现有的大部分公证人跨链方案似乎没有刻意强调跨链安全的问题，仅是通过公证人的可信度、公证人机制的稳定程度保障安全性。但对于公证人选举的过程或者选举出来的公证人账户是否会遭受攻击考虑的很少。因此，如何更好的保护公证人选举的过程，保护选举出来的公证人账户不被泄露，是保证公证人跨链方案安全性的重要部分。

隐私问题：现有的许多公证人跨链方案都特别重视隐私泄露问题，如果在跨链交易过程中所有信息都进行公开，通常无法确保数据隐私和身份隐私的保密性。因此，需要着重考虑采用加密或匿名技术保护跨链交易的隐私性。

可扩展性问题：公证人机制需要公证人节点或机构在不同区块链之间进行通信和协调，但是这可能会增加跨链交易的时间、费用和步骤。因此，如何提高公证人机制的可扩展性，以及如何支持更多类型和数量的区块链系统，是公证人机制需要优化问题。

实现难度问题：相比侧链和中继，传统公证人机制虽然在实现难度较低，但是去中心化程度较低是公证人机制的弊端。面对复杂的需求环境之下，纯公证人机制往往不能在保证拥有较高的去中心化程度的同时，还能较好地应对各种复杂的变化和需求。因此，我们通常还需要增加各种改进措施或者结合其他跨链机制对其进行优化。进行优化的过程中，我们可能需要使用到各种复杂的密码学、共识技术等来实现安全和可靠的跨链交互，这可能会增加开发和部署的技术挑战和复杂度。因此，如何降低公证人机制的实现难度，以及如何提高其可用性和普及性，是公证人机制需要探索的重要问题。

# 5.后续工作

本文对公证人机制进行了详细阐述，对比分析了现有文献提出的基于公证人机制的跨链方案，此外，对公证人机制现存的问题提出了挑战并给出了相应的改进建议。在后续的研究工作中，需要进一步完成以下工作：

(1)对各论文的方法与模型进行进一步的研究。

(2)考虑现有公证人引入改进措施，优化公证人结合哈希时间锁，公证人结合侧链/中继等思路，继续研究基于公证人机制的跨链解决方案。

(3)重点关注公证人机制的隐私性和安全性保护方法。

(4)在公证人安全性和信任问题上，在公证人选举模型优化和公证人签名方式的选择上进行思考；在隐私性问题上，在加密方法上进行思考，从而对公证人机制的跨链解决方案进行突破。

# 参考文献

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Decentralized business review, 2008.
2. Buterin V. A next-generation smart contract and decentralized application platform[J]. white paper, 2014, 3(37): 2-1.
3. Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//Proceedings of the thirteenth EuroSys conference. 2018: 1-15.
4. 周如月, 钱良. 基于区块链信用体系的分布式数字版权管理机制[J]. Application Research of Computers/Jisuanji Yingyong Yanjiu, 2020, 37(6).
5. Xiao X, Leixiao L I, Jing G A O, et al. Research progress of blockchain in internet of vehicles data sharing[J]. Journal of Frontiers of Computer Science & Technology, 2022, 16(5): 1008.
6. Yao Q, Zhang D. Overview of identity management technology in block chain system[J]. J. Softw, 2021, 32: 2260-2286.
7. Abu Bakar Z, Mathews Dr M. A Proposal to Harmonize BIM and IoT Data Silos using Blockchain Application[J]. 2021.
8. Qin K, Gervais A. An overview of blockchain scalability, interoperability and sustainability[J]. Hochschule Luzern Imperial College London Liquidity Network, 2018: 1-15.
9. Dai B R, Jiang S M, Li D, et al. Evaluation model of cross-chain notary mechanism based on improved Page Rank algorithm[J]. Computer Engineering, 2021, 47(2): 26-31.
10. Dai B, Jiang S, Zhu M, et al. Research and implementation of cross-chain transaction model based on improved hash-locking[C]//Blockchain and Trustworthy Systems: Second International Conference, BlockSys 2020, Dali, China, August 6–7, 2020, Revised Selected Papers 2. Springer Singapore, 2020: 218-230.
11. Gaži P, Kiayias A, Zindros D. Proof-of-stake sidechains[C]//2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019: 139-156.
12. Frauenthaler P, Sigwart M, Spanring C, et al. Testimonium: A cost-efficient blockchain relay[J]. arXiv preprint arXiv:2002.12837, 2020.
13. FUSION FOUNDATION. An Inclusive Cryptofinance Plat-form Based on Blockchain[J]. FUSION Whitepaper, 2017
14. Lin S, Kong Y, Nie S. Overview of block chain cross chain technology[C]//2021 13th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA). IEEE, 2021: 357-360.
15. Evans D, Kolesnikov V, Rosulek M. A pragmatic introduction to secure multi-party computation[J]. Foundations and Trends® in Privacy and Security, 2018, 2(2-3): 70-246.
16. Zhang S, Qin B, Zheng H. Research on the protocol of multiple cross-chains based on the hash lock[J]. Information Security and Technology, 2018, 9(11): 57-62.
17. Friedenbach M. Compact spv proofs via block headercommitments[J]. 2014.
18. Timothy D P, Santra A K. A hybrid cryptography algorithm for cloud computing security[C]//2017 International conference on microelectronic devices, circuits and systems (ICMDCS). IEEE, 2017: 1-5.
19. Mamdouh M, Awad A I, Khalaf A A M, et al. Authentication and identity management of IoHT devices: achievements, challenges, and future directions[J]. Computers & Security, 2021, 111: 102491.
20. El Haddouti S, El Kettani M D E C. Analysis of identity management systems using blockchain technology[C]//2019 International Conference on Advanced Communication Technologies and Networking (CommNet). IEEE, 2019: 1-7.
21. Liu L, Xu B. Research on information security technology based on blockchain[C]//2018 IEEE 3rd international conference on cloud computing and big data analysis (ICCCBDA). IEEE, 2018: 380-384.
22. 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.
23. Li T, Yang C, Yang Q, et al. MetaOpera: A Cross-Metaverse Interoperability Protocol[J]. arXiv preprint arXiv:2302.01600, 2023.
24. Wang L, Xie Y, Zhang D, et al. Credible peer-to-peer trading with double-layer energy blockchain network in distributed electricity markets[J]. Electronics, 2021, 10(15): 1815.
25. Cao L, Zhao S, Gao Z S, et al. Cross-chain data traceability mechanism for cross-domain access[J]. The Journal of Supercomputing, 2023, 79(5): 4944-4961.
26. Wu Z, Xiao Y, Zhou E, et al. A solution to data accessibility across heterogeneous blockchains[C]//2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS). IEEE, 2020: 414-421.
27. Wang Z, Li J, Chen X B, et al. A secure cross-chain transaction model based on quantum multi-signature[J]. Quantum Information Processing, 2022, 21(8): 279.
28. Zhao S, Cao L. Dynamic Notary Group Election Algorithm Based on Reputation Value[C]//2022 International Conference on Bigdata Blockchain and Economy Management (ICBBEM 2022). Atlantis Press, 2022: 903-915.
29. 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.
30. Karumba S, Kanhere S S, Jurdak R, et al. HARB: A Hypergraph-Based Adaptive Consortium Blockchain for Decentralized Energy Trading[J]. IEEE Internet of Things Journal, 2020, 9(16): 14216-14227.
31. Yin Z, Zhang B, Xu J, et al. Bool network: An open, distributed, secure cross-chain notary platform[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 3465-3478.
32. Shao S, Chen F, Xiao X, et al. IBE-BCIOT: An IBE based cross-chain communication mechanism of blockchain in IoT[J]. World Wide Web, 2021, 24(5): 1665-1690.
33. Lu S, Pei J, Zhao R, et al. CCIO: A Cross-Chain Interoperability Approach for Consortium Blockchains Based on Oracle[J]. Sensors, 2023, 23(4): 1864.
34. Borkowski M, Sigwart M, Frauenthaler P, et al. DeXTT: Deterministic cross-blockchain token transfers[J]. IEEE access, 2019, 7: 111030-111042.
35. Borkowski M, Ritzer C, Schulte S. Deterministic Witnesses for Claim-First Transactions. 2018[J]. URL: http://dsg. tuwien. ac. at/staff/mborkowski/pub/tast/tast-white-paper-3. pdf. White Paper, Technische Universität Wien. Version, 1.
36. Thomas S, Schwartz E. A protocol for interledger payments[J]. URL https://interledger. org/interledger. pdf, 2015.
37. Dai B, Jiang S, Zhu M, et al. Research and implementation of cross-chain transaction model based on improved hash-locking[C]//Blockchain and Trustworthy Systems: Second International Conference, BlockSys 2020, Dali, China, August 6–7, 2020, Revised Selected Papers 2. Springer Singapore, 2020: 218-230.
38. Yu Y, Zhang S. A Cross-Chain Identify Authentication Scheme Based on Block Chain[C]//2022 3rd International Conference on E-commerce and Internet Technology (ECIT 2022). Atlantis Press, 2022: 635-643.
39. Sun Y, Yi L, Duan L, et al. A Decentralized Cross-Chain Service Protocol based on Notary Schemes and Hash-Locking[C]//2022 IEEE International Conference on Services Computing (SCC). IEEE, 2022: 152-157.
40. Ren Y, Lv Z, Xiong N N, et al. HCNCT: A Cross-chain Interaction Scheme for the Blockchain-based Metaverse[J]. ACM Transactions on Multimedia Computing, Communications and Applications, 2023.
41. Dawei L, Jianwei L, Zongxun T. AgentChain: a decentralized cross-chain exchange system [C]//2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). 2019: 491-498.
42. Hei Y, Li D, Zhang C, et al. Practical AgentChain: A compatible cross-chain exchange system[J]. Future Generation Computer Systems, 2022, 130: 207-218.
43. Jiang Y, Wang C, Wang Y, et al. A cross-chain solution to integrating multiple blockchains for IoT data management[J]. Sensors, 2019, 19(9): 2042.
44. Pang X, Kong N, Chen Z. AbitBridge: A cross-chain protocol based on main-sub-chain architecture[C]//2022 IEEE 5th International Conference on Information Systems and Computer Aided Education (ICISCAE). IEEE, 2022: 99-104.
45. Zhang Y, Hu S, Wang Q, et al. PXCrypto: A Regulated Privacy-Preserving Cross-Chain Transaction Scheme[C]//International Conference on Algorithms and Architectures for Parallel Processing. Cham: Springer Nature Switzerland, 2022: 170-191.
46. Baldimtsi F, Miers I, Zhang X. Anonymous Sidechains[C]//International Workshop on Data Privacy Management. Cham: Springer International Publishing, 2021: 262-277.
47. Deshpande A, Herlihy M. Privacy-preserving cross-chain atomic swaps[C]//International Conference on Financial Cryptography and Data Security. Cham: Springer International Publishing, 2020: 540-549.
48. Shu F, Lei K. Vger: A VRF based cross-chain mechanism for blockchains[C]//Journal of Physics: Conference Series. IOP Publishing, 2021, 1780(1): 012038.
49. 叶祥翮, 刘学业, 王斌辉, 邢树松. 面向联盟链的分布式公证人跨链模型[J]. 应用科学学报, 2022, 40(4): 567-582.
50. Karumba S, Jurdak R, Kanhere S S, et al. Bailif: A blockchain agnostic interoperability framework[C]//2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2023: 1-9.