|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **分类号** |  | **密级** |  | |
|  |  |  |  |  | |
|  | | | | | |
| **重庆邮电大学研究生学位论文**  **开题报告** | | | | | |
|  | | | | | |
|  | **中文题目** | **一种改进的跨链公证人模型研究** | | |  |
|  |  | | |
| **英文题目** | **Research on an improved cross-chain** | | |
|  | **notary model** | | |
| **学 号** | **S221231032** | | |
| **姓 名** | **李江权** | | |
| **学位层次** | **硕士研究生** | | |
| **学位类别** | **工程硕士** | | |
| **学科专业** | **软件工程** | | |
| **研究方向** | **互联网软件与安全技术** | | |
| **指导教师** | **曹岭 副教授** | | |
| **完成日期** | **2023年 12月 10日** | | |
|  | | | |

|  |
| --- |
| **一、选题依据** |
| * 1. **研究背景、目的和意义**   区块链技术，最初由中本聪在2008年提出，并作为(Bitcoin,简称 BTC)[1]的底层技术而闻名于世。作为一种基于密码学原理构建的去中心化、无需信任的分布式数据账本，区块链记录了网络中所有节点间的交易或事件。其共识机制确保了数据的一致性和完整性，使区块链系统不依赖于任何单一实体的控制，具有不可伪造、不可篡改和可追溯等特性。随着比特币、以太坊等加密货币的兴起，区块链已演化为去中心化数字货币和分布式账本技术的核心，广泛应用于云计算、供应链管理、物联网、金融服务、电子政务、数字身份验证、版权保护等众多领域[2]，因此具有巨大的潜力和多样的应用前景。  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。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。跨链技术通过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，能够在一定程度上解决这些挑战，打破不同区块链项目之间的数据孤岛，实现不同区块链之间的互操作性。目前，出现的跨链技术主要包括公证人机制[3]、哈希锁定[4]、侧链/中继[5-6]、分布式私钥控制[7]。虽然这些跨链技术都已经在被应用于各种各样的跨链协议之中，并且取得了许多不错的效果，但是值得一提的是现有的跨链技术都还存在着一些各自的缺点。例如，哈希锁定中可伸缩性和交易时效性的限制的问题、侧链/中继中安全性和侧链维护的问题、分布式私钥控制中私钥管理风险等。公证人机制作为一种主流的跨链技术，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，提供了一个相对简单且灵活的解决方案。然而，这种机制可能导致中心化风险，因为过度依赖中心化的公证人会使整个交易的安全性和可靠性受到威胁。其次，由于引入第三方的作为中介的缘故，公证人机制中将会涉及一些隐私问题。  因此，研究公证人跨链机制中涉及的安全隐私问题，有助于克服现有技术的局限性，推动区块链和跨链技术的发展，具有重要的研究意义。   * 1. **国内外研究现状**   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。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。  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。  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。  分布式签名公证人机制是在多重签名公证人机制上不断优化的具有更高安全性和可靠性的公证人跨链机制。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）[8]的核心思想来保证密钥的安全性和隐私性。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。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。  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  接下来是根据去中心化程度、安全性、隐私性、可扩展性、效率等评估标准，从不同的角度来对它们进行的对比和分析。  **1.2.1 改进的公证人机制**  DeXTT协议[9]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[10]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[10]。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。  Xiong等人[11]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。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。  Vger[12]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。  Wang 等人[13]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。  蒋楚钰等人[14]提出了一种基于公证人组的跨链交互安全模型，模型中将公证人 节点职能分化验证、连接和监督，并分别由不同的角色完成相应职能，由验证组成员打包经过共识的多笔交易成交易组，并利用多重签名技术对它进行签名；然后， 连接者随机选取多笔交易，利用安全多方计算和同态加密等技术判断交易的真实性； 最后，若打包所有符合条件的交易的哈希值真实可靠且被交易验证组验证过，则连 接者可以继续执行多笔跨链交易的批处理任务，并与区块链进行信息交互。  Cao 等人[15]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。  Wu等人[16]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[17]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[18]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。  臧文洋等人[19]提出一种基于门限签名的时间轮换公证人组模型，该模型规定同时在源链和目标链上拥有账户的节点可参与公证人组选拔，通过选拔成为公证人组中的验证节点需缴纳保证金并遵循任期要求，退出的节点位置会被候选公证人组中信用值最高的节点代替。当公证人组验证跨链交易时，采用门限签名方案进行签名，保护验证节点隐私，规定只有超过一半的公证人认证交易合法并签名后，跨链交易才能实施。但是，该模型采用门限签名保护公证人隐私具有强匿名性，将会导致公证人作恶无法被很好的识别的问题。此外，在公证人节点失效时，直接让信誉值最高的公证人进行候补，缺乏公平性，会影响其他候补公证人的积极性。  Tian等人[20]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。  Yin等人[21]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。  **1.2.2 公证人+HTLC**  Dai等人[22]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。  Yu等人[23]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[24]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。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。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。  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[25]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。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。  **1.2.3 公证人+侧链/中继**  AgentChain[26]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[27]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。  叶等人[28]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。  Jiang等人[29]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[30]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[31]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。它设立了单个监管机构，负责对参与交易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。为了保护用户的跨链交易数据隐私[32]，PXCrypto利用代理多方计算机制，通过订单匹配模式来保护订单价格的隐私，并通过监管机构来调节跨链交易结果和进行交易的用户身份。因此，PXCrypto在很大程度上提高了跨链交易的安全性和隐私性。但是，由于引入质押服务商，它同时也牺牲了一定的去中心化程度和灵活性。   * 1. **当前存在的主要问题**  1. **缺乏对公证人有效监管**   当前公证人跨链方案中缺少监管组对公证人有效监管，在这种情况下，将会存在着公证人的违规行为无法及时识别和处理的风险。此外，还可能导致原本诚实的节点因为没有监管而出现违规倾向，进而从事不诚实的行为，例如滥用其职权，进行欺诈或偏袒某方。   1. **验证节点信息公开，缺乏条件隐私保护**   当前公证人跨链方案内，公证人节点往往承担着跨链交易的转发、验证和签署交易等操作，这通常会泄露公证人节点的身份隐私，从而导致公证人遭受针对性攻击或者被伪造签名，这不仅会使得公证节点自身的安全性降低，还会危及整个跨链系统的安全性和稳定性。然而，公证人节点如果完全隐匿其身份进行跨链交易，这又将会助长恶意公证人进行不诚实乃至是违规的行为，因为完全隐匿隐私保护将会使得监管者难以追溯其真实身份，进行扣除押金，从公证人组中清除恶意节点等惩罚。因此，需要未公证人设置相应的可追溯的隐私保护机制，来保障公证人节点和系统的安全性。   1. **公证人管理方案的不足**   当前公证人跨链技术中大多数没有设计候选公证节点或存在候选公证节点参与度不高的问题，缺乏动态和自适应的能力，当公证人节点不及时处理跨链交易时，容易导致交易停滞，从而出现交易资金锁定时间过长、交易超时等问题，缺乏安全性。此外，涉及公证人的信誉、奖惩等管理机制通常只对处理跨链交易公证节点进行评估，而忽视候选公证节点的信誉、奖惩的管理。这可能导致整个公证人社区中只有少数公证节点积极参与跨链交易和系统维护，影响系统的安全性和稳定性。   1. **缺少跨链交易隐私保护**   当前公证人跨链技术中缺少对于跨链交易的隐私保护。公证人跨链技术通过引入第三方节点或机构充当公证人，在跨链交易过程中，交易双方需要将自己的资产交由公证人进行验证、转发、签名等操作。在此跨链交易过程中，交易双方的交易隐私将会被暴露给公证人。然而，交易双方为了保障自身的权益和安全性，在跨链交易过程中并不想暴露这些细节给第三方，这就需要建立一定的隐私保护方法来保护跨链交易的隐私。 |
| **二、研究目标和主要研究内容** |
| **2.1 研究目标**  1、对当前公证人组的管理方案的不足进行改进，提出改进的公证人管理方案，提高候选公证节点的参与度以及公证人的积极性，并且有效降低公证人的作恶行为。  2、优化当前公证人中的监管机制，维护跨链安全性。  3、增强公证人在参与跨链交易过程中的身份隐私保护，避免公证人遭受针对性攻击和被恶意伪造签名。  **2.2 主要研究内容**  **(1) 基于信誉值和投票的公证人管理机制**  设计[基于信誉值和投票的公证人管理机制，根据公证人的跨链交易表现和公证节点的投票行为，动态地调整公证人以及所有候选公证节点的信誉值，以及其在跨链交互中的权重和收益](https://cloud.tencent.com/developer/article/1988295)。通过该管理激励公证人和其他公证节点诚实地履行职责，积极参与跨链系统的维护，防止作弊和攻击，提高跨链交互的效率和安全性。  **(2) 具有监管机制和公证人条件隐私保护的方法**  设立公证人条件隐私保护，在跨链交互中，对公证人的身份、资格、条件等敏感信息进行加密或者匿名化，以防止公证人的身份隐私泄露，从而遭受敌手的识别、勒索或串谋等针对性攻击。此外，监管节点能够对跨链交互的合法性和正确性进行实时或事后的检查，如果发现非法行为，监管小组可以利用手中的密钥碎片，利用分布式秘密共享技术和门限技术恢复公证人的真实身份，系统将对公证人实施扣除押金、剔除公证人组等一系列惩罚。  **(3) 设计基于公证人的跨链交互的系统**  设计基于公证人的跨链资产交互的系统，即通过利用公证人作为中介，实现源链和目标链之间的双向资产锁定和解锁，从而实现不同链之间的价值互通和资产交换。其中，应该考虑在跨链资产交换过程中对于交易者跨链隐私的保护，维护交易者跨链交易的安全性和隐私性。 |
| **三、拟解决关键问题及其研究方法** |
| **3.1 拟解决关键问题**  1、改进现有的公证人的管理方案的不足，引入投票和信誉的公证人管理机制，  优化当前公证人跨链方案内的声誉、奖惩管理机制的缺陷，提高所有候选公证节点和公证人的参与积极性，提高公证人跨链方案动态调整和自适应的能力，维护跨链系统的安全性和稳定性。  2、提出一种具有监管机制和公证人条件隐私保护的方法，从而降低公证人节点在执行跨链交易期间，因身份隐私泄露而遭受针对性攻击、被伪造签名等一系列风险。同时，该方法又能克服过度保护公证人身份隐私，导致公证人违规作恶而无法追溯的问题。  **3.2 采取的研究方法**  1、文献调查法：通过收集、整理、阅读国内外关于区块链互操作性的相关论文，以此来多了解关于基于公证人的跨链机制技术原理以及相关的最新发展状况。  2、对比分析法：基于文献调查法基础之上，对比分析目前公证人跨链机制的优缺点，概括总结现有的公证人跨链机制的水平和研究动态，从中发现当前公证人跨链技术中存在的不足之处。  3、实验验证法：结合现有技术的优点，并从不足之处进行改进优化，设计出新的基于公证人机制的跨链资产交互方案，并且通过相关设备或服务器、利用现有的remix、peersim、适配器等工具进行仿真实验测试。  **3.3 可能的创新**  1、基于信誉值和投票的公证人管理机制  2、具有监管机制和公证人条件隐私保护的方法  **参考文献：（数量不少于30，近三年文献不少于30%，书籍和硕士学位论文不多于30%）**   1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Decentralized business review, 2008. 2. 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). 3. Thomas S, Schwartz E. A protocol for interledger payments[J]. URL https://interledger. org/interledger. pdf, 2015. 4. 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. 5. Gaži P, Kiayias A, Zindros D. Proof-of-stake sidechains[C]//2019 IEEE Symposium on Security and Privacy (SP). IEEE, 2019: 139-156. 6. Frauenthaler P, Sigwart M, Spanring C, et al. Testimonium: A cost-efficient blockchain relay[J]. arXiv preprint arXiv:2002.12837, 2020. 7. FUSION FOUNDATION. An Inclusive Cryptofinance Plat-form Based on Blockchain[J]. FUSION Whitepaper, 2017. 8. 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. 9. Borkowski M, Sigwart M, Frauenthaler P, et al. DeXTT: Deterministic cross-blockchain token transfers[J]. IEEE access, 2019, 7: 111030-111042. 10. 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. 11. 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. 12. 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. 13. 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. 14. 蒋楚钰,方李西,章宁等. 基于公证人组的跨链交互安全模型 [J]. 计算机应用, 2022, 42 (11): 3438-3443. 15. 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. 16. 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. 17. 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. 18. 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. 19. 臧文洋,吕进来. 基于门限签名的时间轮换公证人组模型研究 [J/OL]. 计算机科学, 1-14[2023-12-21] 20. 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. 21. 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. 22. 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. 23. 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. 24. 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. 25. 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. 26. 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. 27. 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. 28. 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. 29. 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. 30. 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. 31. 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. 32. Yin R, Yan Z, Liang X, et al. A survey on privacy preservation techniques for blockchain interoperability[J]. Journal of Systems Architecture, 2023, 140: 102892. |
| **四、进度安排和预期成果** |
| **4.1 预期成果**  根据研究内容发表学术论文 1 篇或发明专利受理 2 篇  **4.2 进度安排**   |  |  |  | | --- | --- | --- | | 时间段 | 工作内容 | 预期成果 | | 2024.01-2024.04 | 完善基于信誉值和投票的公证人管理机制，设计相关的算法和协议 | 形成成熟的公证人管理机制 | | 2024.04-2024.06 | 设计监管机制和身份隐私保护的公证人方法 | 形成成熟的公证人身份隐私保护方法 | | 2024.06-2024.10 | 搭建跨链系统和测试环境，进行仿真、模拟实验，进行实验验证 | 完成实验的初步验证，解决存在的问题 | | 2024.10-2024.12 | 对初步的实验结果进行分析与优化，准备中期答辩 | 得出分析与优化的结果，准备中期答辩的材料 | | 2025.01-2025.05 | 根据优化结果，进行最终验证，完成毕业论文的撰写工作，准备毕业论文的相关材料 | 论文撰写完成，进行毕业答辩 |   **4.3 研究条件**  软件条件：Windows10 64bit, Ubuntu 18.04，IntelliJ IDEA 2023.2.3，Visual Studio Code, GoLand 2023.1.3，Docker，Remix  文献资料：学校图书馆数据库的 IEEE、ACM 等数据库，SCI、EI 等索引数据库以及Google学术等搜索引擎。  硬件设备: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHZ RAM 12.0 GB笔记本一台  老师及实验室：导师曹岭副教授作为实验室的领导者，拥有多年的区块链研究经验和深厚的学术造诣，能够在关键的时刻给出有效的建议和意见，避免在研究过程中出现走过多弯路。实验室内部设有研究讨论会和学术指导会，可以和其他同学之间深入交流学术知识和实验进展，这有助于提升学术水平，促进研究项目的顺利进行。实验室拥有先进的硬件设备和软件工具，以支持各种学术研究的进行。  因此，经本人与导师共同分析，具备支持论文研究的条件。 |

备注：以上内容根据情况添页。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **论文开题管理** | | | | | |
| 版本说明 | 提交版本：首次提交/二次提交。  如非首次提交，说明本次提交的修改内容。 | | | | |
| 学生承诺 | 学生签字： 年 月 日 | | | | |
| 导师意见 | 导师签字： 年 月 日 | | | | |
| 开  题  组  成  员 |  | 姓 名 | 职 称 | | 所 在 单 位 |
| 组 长 |  |  | |  |
| 成 员 |  |  | |  |
| 成 员 |  |  | |  |
| 成 员 |  |  | |  |
| 成 员 |  |  | |  |
| 开  题  报  告  组  意  见 | 组长签字： 年 月 日 | | | | |
| 导师团队意见 | 负责人： 年 月 日 | | | 学院意见 | 院长： 年 月 日 |

备注：本页单独打印在一页。