基于门限签名的时间轮换公证人组模型研究

臧文洋，吕进来

引用本文

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]. 计算机科学，2024，51(8)：403-411.

ZANG Wenyang, LYU Jinlai. Study on Time Rotation Notary Group Model Based on Threshold Signature [J]. Computer Science, 2024, 51(8): 403-411.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230500060

基于门限签名的时间轮换公证人组模型研究

臧文洋　吕进来
太原理工大学信息与计算机学院　山西 晋中 030600
(945866542@qq.com)

摘　要　随着各类区块链系统的不断涌现,跨链交互需求不断增加,跨链桥验证环节的安全性显得愈发重要。公证人机制原理简单、效率较高,常用于跨链交易验证、跨链交易确认等环节。但公证人机制存在去中心化程度低、低签名比例可验证交易、验证节点信息公开等问题。为提高跨链桥验证环节的安全性,提出了一种基于门限签名的时间轮换公证人组模型。该模型中的公证人组由同时拥有源区块链和目标区块链账户的高信用值节点组成。公证人组中的验证节点有任期要求且需质押保证金,公证人组采用门限签名技术对跨链交易进行签名,一半以上的验证节点签名后,跨链交易才能实施;候选公证人组为时间轮换公证人组提供新验证节点。分析结果表明,所提模型去中心化程度高,验证节点恶意攻击率低,验证签名环节安全性高,验证节点私密性高,跨链消息验证效率高。

关键词:区块链;跨链;跨链桥;公证人机制;门限签名
中图分类号　TP309

Study on Time Rotation Notary Group Model Based on Threshold Signature

ZANG Wenyang and LYU Jinlai
School of Information and Computer,Taiyuan University of Technology,Jinzhong,Shanxi 030600,China

Abstract　With the emergence of various blockchain systems,the demand for cross-chain interaction is increasing,and the security of cross-chain bridge verification becomes more and more important. The notary schemes have simple principle and high efficiency,and are often used in cross-chain transaction verification,cross-chain transaction confirmation and other processes. However,the notary schemes have some problems,such as low degree of decentralization,verifiable transactions with low signature ratio,and information disclosure of verification nodes. In order to improve the security of cross-chain bridge verification,a time rotation notary group model based on threshold signature is proposed. The notary group in this model is composed of high credibility nodes that have both source and target blockchain accounts. The verification nodes in the notary group have tenure requirements and need to pledge the security deposit. The notary group uses threshold signature technology to sign cross-chain transactions. The cross-chain transaction can only be implemented after more than half of the verification nodes in the notary group sign. The candidate notary group provides some new verification nodes for the time rotation notary group. The analysis results of the time rotation notary group model proves that the proposed model has high degree of decentralization,low malicious attack rate of the verification nodes,high security of the verification signature links,high privacy of the verification nodes,and high efficiency of cross-chain message verification.

Keywords　Blockchain,Cross-chain,Cross-chain bridge,Notary schemes,Threshold signature

1　引言

随着比特币(Bitcoin,数字货币代码 BTC)[1]、以太坊(Ethereum,数字货币代码 ETH)[2]、币安币(Binance Coin,数字货币代码 BNB)、瑞波币(Ripple,数字货币代码 XRP)[3]等数字加密货币的流行,区块链[1]受到多方关注,并得到快速发展。区块链具备不可伪造、不可篡改、匿名化、去中心化、可追溯的优点,基于这些优点,区块链受到金融、司法、医疗、版权等多个领域的青睐,并逐渐应用于各个领域,例如招商银行开发的"招商银行一链通"区块链技术平台以及微众银行的产品——微众区块链已成功支持金融、司法、医疗等多个领域数以百计的区块链应用落地。截至 2023 年 1 月 12 日,Github 中与区块链相关的代码库已有 156 576 个,相关用户有 31 531 位,足以说明区块链领域正在蓬勃发展。

随着区块链技术、共识算法[4]的不断优化发展,各形各色的联盟链(Consortium Blockchain)[5]、公有链(Public Blockchain)[6]以及私有链(Private Blockchain)[7]不断涌现。联盟链中只有被授权的节点才能根据权限读取数据、发送交易、参与共识、加入或退出网络,如 Hyperledger Fabric[8]。公有链允许任何节点读取数据、发送交易、参与共识,无需许可即可

到稿日期:2023-05-09　返修日期:2023-10-11
通信作者:吕进来(lujlsx@163.com)

随时加入或退出网络，如比特币。私有链是对单独的实体或个人开放，任何节点的加入、读取数据等操作权限都需要系统权限的管理者给予。这些区块链系统大多互不相通，因此，区块链系统数量越多，价值孤岛现象就越严重。目前，区块链已进入区块链 3.0 时代[9]，其面临的业务需求愈加复杂，跨链交互需求随之增加。将同构或异构的区块链互联互通，形成一个去中心化的链联网（Internet of Blockchains，IoB）[10]，实现区块链之间的数据交互、资产（价值）交互、功能（智能合约）交互。跨链技术在其中发挥了很大作用。跨链桥作为跨链的基础设施，实现了同构或异构区块链之间的交互，但同时也成为黑客攻击的目标，导致了巨大的经济损失。2022 年上半年，在 4 件损失上亿美元的安全事件中有 3 件与跨链桥相关。2022 年，10 件损失最大的安全事件中有 5 件与跨链桥相关。2022 年，12 件与跨链桥相关的安全事件，损失金额共计约 18.9 亿美元，居所有安全事件类型中的第一位。2022 年，由跨链桥的验证环节导致的损失约为 10.5 亿美元，占跨链桥损失金额一半以上，因此，提升跨链桥验证环节的安全性迫在眉睫。

公证人机制（Notary Schemes）[11]原理简单、易于实现、运行效率相对较高，常用于跨链资产转移、跨链资产抵押、跨链交换等多种场景。目前，已有多位学者对公证人机制进行研究和改进。对于公证人机制中节点信用监督不足的问题，Dai 等[11]基于改进的 PageRank 算法，提出公证人节点信用评价模型，此模型利用改进的 PageRank 算法求得公证人节点的信用值，将信用值较低的公证人节点剔除，以保障跨链安全。对于公证人机制跨链交互效率低、节点职能集中的缺点，Jiang 等[12]基于公证人组，提出跨链交互安全模型，此模型将公证人节点划分为交易验证者、连接者和监督者，每类节点只需完成本职工作，在提升跨链交互效率的同时，保障了数据完整性和信息机密性。针对联盟链存储资源浪费的问题，Ye 等[5]提出了一种分布式公证人跨链模型，此模型从各局部链中选举节点组成全局链，在提升系统存储空间利用率的同时，提高了模型的去中心化程度。为避免委员会串谋作恶，Xu 等[13]设计了委员会选举和轮换算法，提高了委员会中节点的去中心化程度和委员会可信度。

目前公证人机制依然存在以下问题：1）公证人机制中心化程度相对较高，公证人一旦被攻击，跨链资产安全就会受到威胁；2）公证人机制对验证交易的公证人签名比例没有明确规定，如果较低的签名比例就可以验证交易，则交易的安全性就会降低，例如 Horizon 跨链桥规定只要获得 5 个多签地址中的 2 个地址签名就可以成功验证交易，由于只需要不到一半比例的签名即可验证交易，因此导致上亿美元的损失；3）验证节点信息是公开的，这就方便了黑客攻击验证节点，伪造签名获取跨链资产。

为解决以上问题，本文提出了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。时间轮换公证人组模型的分析结果表明，所提模型去中心化程度高，恶意攻击率低，跨链交易验证环节安全性高，验证节点的选举和签名效率较高。本文的主要贡献如下：

1）设计时间轮换公证人组选举方案和任期管理方案，提高了公证人组的去中心化程度。

2）引入改进的 PageRank 算法筛选节点，提升了验证节点信用度；设计保证金管理方案，降低了验证节点恶意攻击率。

3）引入门限签名方案对跨链交易进行签名，提高了验证节点的私密程度；设定签名比例，提升了验证签名环节的安全性。

4）设计候选公证人组，为时间轮换公证人组输送新的验证节点，提升了验证节点的选举效率；与多重签名相比，所提算法提高了验证签名效率，降低了签名手续费。

本文第 2 章介绍跨链和跨链桥的相关内容，包括跨链和跨链桥的概念、技术方案、黑客攻击事件；第 3 章介绍时间轮换公证人组模型设计；第 4 章对时间轮换公证人组模型的安全性和效率进行分析证明；最后总结全文并展望未来。

2 跨链和跨链桥简介

2.1 跨链

跨链（Cross-chain），即通过跨链技术，使数据、资产、功能（智能合约）能够在同构或异构的区块链间交互流通。在跨链过程中，跨链技术是关键，跨链技术指能让同构或异构区块链实现价值交互、信息相通的技术[14]。当今常用的跨链技术有 4 种，分别是公证人机制、侧链/中继（Sidechains/Relays）[15]、哈希锁定（Hash-locking）[16]、分布式私钥控制（Distributed Private Key Control）[17]。

公证人指公正独立可信任的第三方，相当于中介。公证人机制指借助公正独立可信任的第三方来验证跨链交易是否合规合法。按照签名形式的不同，公证人机制可分成中心化公证人机制、多重签名公证人机制和分布式签名公证人机制 3 类。

中心化公证人机制只需单个公证人即可进行信息交互、跨链交易验证等工作，因此中心化公证人机制的运行效率相对较高。若公证人受到袭击，则公证人不可信、跨链交易不可信、系统出现单点故障，因此中心化公证人机制的安全性相对较低。

多重签名公证人机制[18]需要多位公证人协同参与完成交易验证等工作。唯有满足规定比例或数量的公证人达成共识、完成签名，才能够成功实施跨链交易。与中心化公证人机制相比，多重签名公证人机制去中心化程度更高，具有更高的安全性。

分布式签名公证人机制同样要求多位公证人协同开展交易验证等工作。分布式签名公证人机制中的公证人选用多方计算 MPC 思想[19]完成签名工作。与多重签名公证人机制相比，分布式签名公证人机制安全性更高，同时更复杂，实现难度较大。

侧链是一条小型区块链，主要附着在主链旁边。侧链能够接收并读取主链信息，包括主链交易数据、交易地址等。通过锚定的方法，主链和侧链可进行双向跨链交易。跨链过程中

资产并没有在主链和侧链间转移，而是资产锁定和释放。在以太坊基金会的支持下，区块链中首个侧链 BTC Relay[20] 诞生。BTC Relay 借助以太坊网络中的智能合约，将比特币网络和以太坊网络衔接起来，打通了不同区块链间交流的通道。

中继链宛如公证人机制和侧链的融合体，它能够作为第三方公证人成为不同区块链的信息中心，完成读取、收集并查验不同区块链间的跨链交易信息。侧链从属于主链，和主链关系亲密。中继链不属于任何区块链，与其他区块链是平等、平行的关系，这是中继链和侧链的最大区别。

哈希锁定又被称为哈希时间锁定，起源于 Lightning network 闪电网络[21] 的 Hashed TimeLock Contract，简称 HTLC。哈希锁定通过哈希锁和时间锁实现交易的原子性。哈希时间锁锁定源链上的资产，源链随机生成数字 S，将随机数 S 的哈希值 H 发送给目标链，目标链在规定时间内提供能生成哈希值 H 的随机数 S，则在目标链上释放等价值的资产，完成跨链。否则源链上的资产自动解锁，返还给原本拥有者。

分布式私钥控制指创建被不同节点、组织或者机构保存的一组私钥，用于掌管用户资产。通过这组私钥可以对资产进行锁定和解锁操作。锁定指收回用户对源链资产的控制权，用户只能控制在目标链上铸造封装的等额资产。解锁是将源链资产的控制权还给用户，用户可以对源链资产进行转移和跨链等操作。通过分布式私钥控制可以实现去中心化，保护跨链资产的安全。

2.2 跨链桥

跨链桥是跨链所需的基础设施，由协议和技术组成。通过跨链桥，区块链间可以互联互通，能够进行数据、资产的交互。跨链桥分为任意消息跨链桥（Arbitrary Message Bridge，AMB）和资产跨链桥。资产跨链桥可分为封装代币桥（wrap 桥）和流动性兑换桥（swap 桥）。跨链桥的跨链方案包括锁定＋铸造、销毁＋铸造、原子转移（Atomic Transfers）[22]、流动性池。

锁定＋铸造包括源链资产锁定、目标链资产铸造和目标链资产销毁、源链资产解锁两大环节。资产的锁定、铸造、销毁、解锁操作均依赖于智能合约或者资产托管地址的第三方组织、机构或节点，智能合约或资产托管地址的第三方出现漏洞，会直接影响跨链资产安全。

销毁＋铸造包括源链资产销毁、目标链资产铸造和目标链资产销毁、源链资产铸造两大环节。资产的销毁和铸造操作依赖于智能合约或者资产托管地址的第三方组织、机构或节点，智能合约或资产托管地址的第三方出现漏洞，会直接影响跨链资产安全。锁定＋铸造和销毁＋铸造与原子转移和流动性池相比，跨链交易步骤较多，因此跨链效率相对较低。

原子转移又被称为原子交换（Atomic Swap）。原子转移无需锁定、铸造或销毁资产，而是通过智能合约机制，直接转换源区块链和目标区块链上的资产。原子转移要求源链和目标链遵循的算法一致，且均支持哈希时间锁定。原子转移要求通过密钥对资产进行存取操作，若某一方违规操作，则另一方可利用时间锁拿回自己的资产，不需要将资产托付给第三方，因此安全性更高且更加去中心化。满足原子转移要求的源区块链和目标区块链上的所有资产都能直接进行跨链交易，无需第三方参与，因此跨链交易效率高且费用低。

流动性池被事先创建在源区块链和目标区块链上。源区块链流动性池和目标区块链流动性池需事先放置好资产，以供跨链交易使用，因此需要给予流动性提供者奖励。但也正因为事先在流动性池中放置了资产，因此与锁定＋铸造和销毁＋铸造相比，流动性池跨链交易效率更高。流动性池不需要第三方参与即可进行跨链交易，因此与锁定＋铸造和销毁＋铸造相比去中心化程度更高。流动性池的安全十分重要，若流动性池被攻击，则流动性池中的流动性资金很有可能被盗取，流动性池失去平衡会导致跨链资产凭空消失，进而将危机传给用户。当存在大量的单向跨链交易时，流动性池很有可能会耗尽，这是流动性池的缺点所在。

2.3 跨链桥黑客攻击事件

2022 年黑客攻击跨链桥验证环节的典型事件有 3 起。

2022 年 2 月 2 日，跨链桥虫洞协议 Wormhole Protocal 遭到黑客袭击，黑客攻击 Wormhole 在 Solana 一侧的漏洞，绕过签名检查合约，获得所需参数，凭空铸造并盗取 12 万枚 ETH，价值约 3.26 亿美元。

2022 年 3 月 23 日，Ronin Network 受到黑客袭击，黑客主要攻击 4 个私钥，制造 5 个合法签名，利用签名伪造提款证明，共窃取 2 550 万枚 USDC 和 17.36 万枚 ETH，总价值约 6.24 亿美元。该事件是跨链桥迄今为止损失最大的黑客袭击事件。

2022 年 6 月 24 日，Horizon 跨链桥受到黑客袭击，黑客成功攻击 2 个多签地址，获得 2 个地址私钥，进而签署验证一些非法交易。被盗取的货币包括 WETH，AAVE，SUSHI，DAI，USDT，USDC，价值约 1 亿美元。

3 时间轮换公证人组模型设计

本文提出的时间轮换公证人组模型是在同时拥有源区块链和目标区块链账户的可信节点集合中，按比例选取一组信用值高的节点组成公证人组。公证人组中的验证节点有任期要求，超过任期的验证节点会失效，此时需在候选公证人组中重新选取信用值最高的节点替换失效的验证节点。公证人组中的验证节点需要质押保证金，如果验证节点违规操作或成为恶意节点，则没收此验证节点的保证金，进而降低验证节点恶意攻击率。时间轮换公证人组模型采用门限签名方案（Threshold Signature Schemes，TSS）[23] 进行签名工作，隐藏参与验证签名的节点信息，提高验证节点的私密度。当验证跨链交易时，需要公证人组中一半以上的验证节点认证交易合法并签名后，跨链交易才能实施，以此提升黑客攻击的难度和跨链桥验证环节的安全性。除了时间轮换公证人组中的验证节点和刚失效的验证节点，候选公证人组中的节点是信用值最高的一组节点，可直接为时间轮换公证人组提供新的验证节点，节省验证节点选举轮换时间，提升时间轮换公证人组的跨链消息验证效率。

本章将从跨链网络模型、跨链步骤、时间轮换公证人组的管理 3 方面来阐述时间轮换公证人组模型。

3.1 跨链网络模型

时间轮换公证人组模型的跨链网络模型由源区块链、目标区块链和时间轮换公证人组构成。跨链网络模型示意图如图 1 所示。

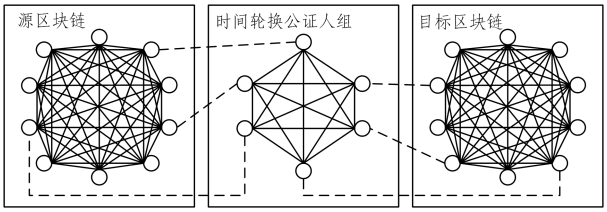

图 1 跨链网络模型

Fig. 1 Cross-chain network model

源区块链中有多个节点，节点会存储链中的交互信息，并采用共识算法抢夺记账权。获得记账权的节点将某一时期内的交互信息打包广播，让其他节点存储的交互信息与之同步，保证链中信息的一致性和完整性。同理，目标区块链中也有多个节点，节点也会存储链中的交互信息，并采用共识算法抢夺记账权。获得记账权的节点将某一时期内的交互信息打包广播，让其他节点存储的交互信息与之同步，保证链中信息的一致性和完整性。源区块链中的用户只需访问本链节点即可获得本链中的信息，若要与目标区块链交互信息，则需要进行跨链操作。

时间轮换公证人组负责验证传递源区块链和目标区块链之间的交互信息。同时拥有源区块链和目标区块链账户的节点可参与时间轮换公证人组的选拔，采用改进的 PageRank 算法按比例选取信用值最高的一组节点组成时间轮换公证人组。公证人组中的验证节点需缴纳保证金并有任期要求，若某验证节点任期已至且没有正在进行的验证工作，则此失效验证节点的位置将被候选公证人组中信用值最高的节点代替。从源区块链和目标区块链中选取的高信用值节点组成的时间轮换公证人组验证传递的跨链交互信息能被源区块链和目标区块链所信任。

3.2 跨链步骤

3.2.1 任意消息跨链步骤

任意消息跨链中包含消息请求者、时间轮换公证人组、消息提供者 3 个角色。以数据跨链为例，当源区块链想获取目标区块链的某个数据时，数据跨链流程如图 2 所示，数据跨链的具体步骤如下。

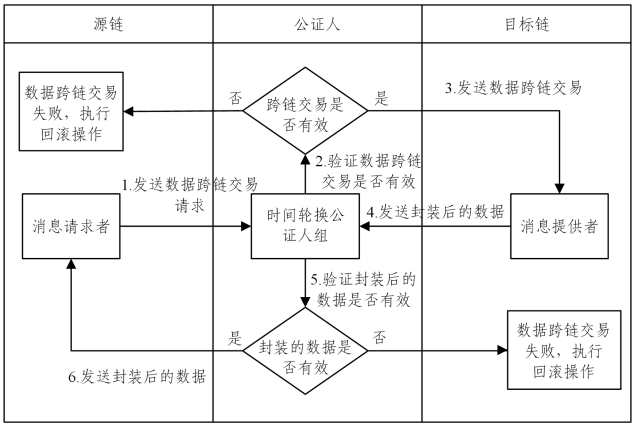

图 2 数据跨链流程

Fig. 2 Data cross-chain process

步骤 1 消息请求者将数据跨链交易请求发送给时间轮换公证人组。

步骤 2 时间轮换公证人组通过监测源区块链，验证数据跨链交易的有效性，若交易有效，则进行步骤 3；若交易无效，则执行 rollback 回滚操作。

步骤 3 时间轮换公证人组将数据跨链交易封装后发送给消息提供者。

步骤 4 消息提供者处理数据跨链交易，整合消息请求者所需数据，将数据封装后发送给时间轮换公证人组。

步骤 5 时间轮换公证人组通过监测目标区块链，对消息提供者发送的数据进行验证。若数据有效，则进行步骤 6，否则执行 rollback 回滚操作。

步骤 6 时间轮换公证人组将数据发送给源区块链中的消息请求者。

3.2.2 资产跨链步骤

资产跨链中包含用户在源链上的地址、源链智能合约、时间轮换公证人组、目标链智能合约，以及用户在目标链上的地址 5 个角色。以锁定＋铸造资产为例，资产跨链流程如图 3 所示，资产跨链的具体步骤如下：

步骤 1 用户在源链上的地址发起资产跨链请求，并将资产发送给源链智能合约。

步骤 2 源链智能合约锁定资产，并给用户在源链上的地址返回资产跨链请求日志。

步骤 3 用户在源链上的地址请求时间轮换公证人组验证资产跨链请求日志。

步骤 4 时间轮换公证人组通过监测源区块链，检查源链资产是否锁定在源链智能合约中。如果用户在源链上的资产确实锁定在源链智能合约中，则进行步骤 5；若资产未锁定在源链智能合约中，则资产跨链失败，执行 rollback 回滚操作。

步骤 5 时间轮换公证人组对“用户锁定资产”交易签名，并将签名返回给用户在源链上的地址。

步骤 6 用户在源链上的地址将“用户锁定资产”交易签名和资产跨链信息封装后发送给目标链智能合约。

步骤 7 目标链智能合约收到交易签名和资产跨链信息后，向时间轮换公证人组求证签名和源链资产跨链信息的真实性。若签名为真，且源链资产跨链信息无误，则记录源链资产跨链交易信息，执行步骤 8；否则资产跨链失败，执行 rollback 回滚操作。

步骤 8 目标链智能合约铸造与用户锁定资产等值的资产，发起将铸造资产转移到用户在目标链上规定地址的交易。当这笔交易得到目标区块链的验证并写入目标区块链后，用户在目标链上的地址即可收到铸造资产。

步骤 9 用户在目标链上的地址收到铸造资产后，向目标链智能合约返回资产跨链成功日志。

步骤 10 目标链智能合约请求时间轮换公证人组验证资产跨链成功日志。

步骤 11 时间轮换公证人组通过监测目标区块链，验证资产跨链成功日志的真实性。若资产跨链成功日志为真，则将日志发送给用户在源链上的地址，否则执行 rollback 回滚操作。

若用户想要赎回被源链智能合约锁定的资产，则目标链

智能合约需先销毁铸造封装的资产，经时间轮换公证人组确认销毁后，用户才可赎回源链锁定的资产。

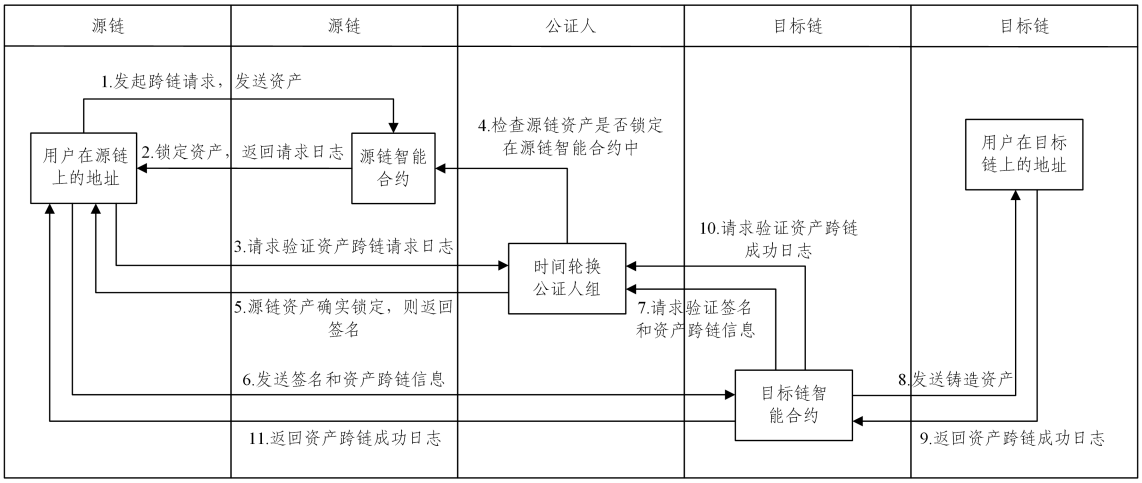

图 3 资产跨链流程

Fig. 3 Asset cross-chain process

3.3 时间轮换公证人组的管理

时间轮换公证人组的管理包括建立时间轮换公证人组、加入时间轮换公证人组、验证节点的任期管理、管理保证金、设计签名方案和退出时间轮换公证人组 6 个方面。

3.3.1 建立时间轮换公证人组

只有同时拥有源区块链账户和目标区块链账户的节点才可申请参加时间轮换公证人组的选举过程。时间轮换公证人组的建立总共分为三大步骤：构建可信任集合 P、构建时间轮换公证人组 T、构建候选公证人组 G。

1）构建可信任集合 P

引入 Dai 等提出的改进 PageRank 算法对同时拥有源区块链和目标区块链账户的节点进行信用值排序，将低于信用值门槛的节点剔除，剩余节点按信用值由高到低排序组成可信任集合 P。

可信任集合 P 中的节点在加入 P 之前需要经过改进 PageRank 算法审核筛选，以降低 P 中恶意节点的概率。P 中的节点在源链和目标链上均有账户，若 T 中属于源链的节点联合作恶，损害目标链的利益，则作恶节点在目标链上的账户也会受到波及，反之亦然。因此，从属于一条链的节点联合作恶的概率较低。

2）构建时间轮换公证人组 T

从集合 P 中按比例优先选取信用值高的 m_1 个源链节点和 m_2 个目标链节点组成时间轮换公证人组 T，以此提升时间轮换公证人组的可信度。为防止 T 中验证节点中心化，源链和目标链中都必须至少选出一个属于时间轮换公证人组的节点，即 m_1 和 m_2 的最小值为 1。

设公证人组 T 中验证节点数量为 m，源链上的节点数量为 n_1，目标链上的节点数量为 n_2，则 m_1 和 m_2 的值为：

$$m_1=\frac{n_1}{n_1+n_2}\times m,1\leqslant m_1\leqslant m-1$$

$$m_2=\frac{n_2}{n_1+n_2}\times m,1\leqslant m_2\leqslant m-1$$

若有一些恶意节点乔装成可信任节点成功加入时间轮换公证人组 T 中，它们仍旧需要遵循拜占庭容错机制，即 T 中最多有 1/3 的节点为恶意节点。由于 T 中节点有任期要求，因此 1/3 的恶意节点同一时间内出现在 T 中的概率较小。T 中需要一半以上的验证节点签名才能成功验证并签署跨链交易，因此即使 T 中同时出现 1/3 的恶意节点联合作恶，也无法签署非法交易。

3）构建候选公证人组 G

将集合 P 中除 T 中验证节点以外的节点组成候选公证人组 G。候选公证人组 G 中的节点是除了 T 中验证节点和刚失效的验证节点以外，信用值最高的一组节点。因此，对于举报，候选公证人组可核实举报内容的真假，对于退出 T 的验证节点，可以直接从 G 中选出信用值最高的节点替补其位置。

3.3.2 加入时间轮换公证人组

加入时间轮换公证人组的方式有两种，分别是正常加入和异常加入。

1）正常加入

若当前时间轮换公证人组中的某个验证节点任期已至，且该验证节点没有正在进行的跨链交易验证工作，则该验证节点失效，候选公证人组中信用值最高的节点替补失效验证节点的位置，组成新一轮的时间轮换公证人组。

由于时间轮换公证人组中的验证节点不能连任，因此失效的验证节点不能参与本轮时间轮换公证人组验证节点的选拔，只能重新计算信用值，参与下一轮时间轮换公证人组验证节点的选拔。

2）异常加入

当时间轮换公证人组中的某个验证节点任期未至，但想主动退出时间轮换公证人组时，候选公证人组中信用值最高的节点将代替主动退出的验证节点，组成新一轮的时间轮换公证人组。

当时间轮换公证人组中的验证节点 A 举报验证节点 B 违规操作或成为恶意节点，此时候选公证人组中的节点会对验证节点 B 的性质进行验证。若 A 举报属实，则验证节点 B 被时间轮换公证人组剔除，候选公证人组中信用值最高的节点将替补验证节点 B 的位置，组成新一轮的时间轮换公证人组。若验证节点 A 恶意举报，则验证节点 A 存在违规操作，

此时验证节点 A 被时间轮换公证人组剔除，候选公证人组中信用值最高的节点将替补验证节点 A 的位置，组成新一轮的时间轮换公证人组。

3.3.3 验证节点的任期管理

由于时间轮换公证人组中的验证节点难以长时间维持较高的信用值，因此时间轮换公证人组中的验证节点有任期要求，且所有验证节点的任期一致。

任期管理中最重要的是任期期限设置。任期过短，会导致恶意节点被举报的同时其任期已至，此时候选公证人组还未验明恶意节点的身份、保证金未来得及罚没，恶意节点就成功离开。任期过长，黑客则有足够时间攻击验证节点，签署非法交易。因此时间轮换公证人组采用纪元边界中定义的 12 s 时间槽作为 T 中验证节点的任期期限。

时间轮换公证人组采用 TSS 方案进行签名工作，参与验证的节点信息被隐藏。黑客在 12 s 内找出验证节点的概率较低，即使找到验证节点，黑客也需在节点任期内成功攻击一半以上的验证节点才能签署非法交易，而且在黑客攻击过程中，时间轮换公证人组中的验证节点会随时间变化而变化。因此，在 12 s 内黑客成功攻击时间轮换公证人组的概率极低。

若时间轮换公证人组中某验证节点任期已至且没有正在进行的验证工作，则此验证节点失效。除时间轮换公证人组中的验证节点和刚失效的验证节点外，信用值最高的一组节点均处于候选公证人组中，因此可以直接从候选公证人组中选取信用值最高的节点代替失效节点的位置，时间轮换公证人组中其余未失效的验证节点无需被替换。与替换时间轮换公证人组中所有节点相比，仅替换失效验证节点可以提高选举效率。直接从候选公证人组中选取信用值最高的节点可节省选举时间，提高选举效率。

3.3.4 管理保证金

加入时间轮换公证人组的验证节点都需要缴纳保证金，以质押保证金的方式，降低验证节点恶意攻击率。

当验证节点正常退出公证人组时，将退还验证节点缴纳的保证金。当验证节点主动退出公证人组时，将被扣除一定比例的保证金，用于奖励临时被选中来代替它身份的新验证节点。当验证节点被动退出公证人组时，其缴纳的保证金将被全额没收。没收的保证金将用于奖励参与举报过程的验证节点，或弥补用户损失，亦或支付时间轮换公证人组中验证节点的酬劳。

当时间轮换公证人组中的验证节点 A 举报验证节点 B 违规操作或成为恶意节点，此时候选公证人组中的验证节点会对验证节点 B 的性质进行验证。若 A 举报属实，则没收验证节点 B 的保证金，奖励给参与举报过程的验证节点，包括验证节点 A 和候选公证人组中的验证节点。若验证节点 A 恶意举报，则验证节点 A 存在违规操作，此时没收验证节点 A 的保证金，奖励给候选公证人组中的验证节点。若公证人组中没有节点发现验证节点 B 违规操作或成为恶意节点，且验证节点 B 造成用户损失，则没收验证节点 B 的保证金并补偿给用户；若没有造成用户损失，则没收验证节点 B 的保证金用于支付验证节点的酬劳。

3.3.5 设计签名方案

为保护时间轮换公证人组中验证节点的隐私，时间轮换公证人组采用门限签名方案完成签名工作。签名方案流程如图 4 所示，包含系统初始化、生成公私钥、生成签名和验证签名 4 个环节。

1)系统初始化

确定时间轮换公证人组的规模 n 和门限值 t 的数值，n 和 t 均为正整数，且 t 小于 n。椭圆曲线生成元为 G，阶为 $|F_r|$，标量域为 F_r，基域为 F_q，安全参数为 λ。

2)生成公私钥

时间轮换公证人组中的 n 个验证节点 P_i 各自选择随机数 $u_i \in F_r$，计算 $U_i := u_i \cdot G$，$(KGC_i, KGD_i) = Com(U_i)$，广播 KGC_i 和广播 KGD_i。校验承诺正确性后，计算公共公钥 $PK = \sum_{i=1}^{n} U_i$。

n 个验证节点 P_i 在 F_r 中各自选择 $t-1$ 个随机数 $a_{i,j}$ 构造如下所示的 $t-1$ 阶多项式：$p_i(x) = u_i + a_{i,1} \cdot x + a_{i,2} \cdot x^2 + \cdots + a_{i,t-1} \cdot x^{t-1}$，其中 $i = 1, 2, \cdots, n$；$j = 1, 2, \cdots, t-1$。存储 $p_i(i)$，将 $p_k(k)$ 保密发送给 P_k，其中 $k = 1, 2, \cdots, n$；$k \neq i$。

验证节点 P_i 计算并广播校验元组 $A_{i,j} := a_{i,j} \cdot G$，$j = 1, 2, \cdots, t-1$。

验证节点 P_i 对收到的校验元组进行校验 $p_z(i) \cdot G == U_z + \sum_{j=1}^{t-1} A_{i,j}$，$z = 1, 2, \cdots, n$。

计算验证节点 P_i 的分片私钥 x_i：

$$x_i := \sum_{z=1}^{n} p_z(i) \bmod n = \sum_{z=1}^{n} (u_z + \sum_{j=1}^{t-1} a_{z,j}) \bmod n, \sum_{z=1}^{n} (u_z + \sum_{j=1}^{t-1} a_{z,j}) = sk + \sum_{z=1}^{n} (\sum_{j=1}^{t-1} a_{z,j}) \bmod n$$

计算并广播验证节点 P_i 的分片公钥 X_i：

$$X_i := PK + G \cdot \sum_{z=1}^{n} (\sum_{j=1}^{t-1} a_{z,j})$$

公共公钥 PK 和分片公钥 X_i 之间满足 $PK == \sum_{i=1}^{n} (\lambda_i \cdot X_i)$，公共私钥 sk 和分片私钥之间满足 $sk == \sum_{i=1}^{n} (\lambda_i \cdot x_i)$。$sk = \sum_{i=1}^{n} w_i$，其中 w_i 被称为私钥加性份额。验证节点无需重构公共私钥 sk，而是基于私钥加性份额 w_i 生成签名加性份额 sig_i，将签名加性份额累加即可得到完整签名。

时间轮换公证人组中所有验证节点均拥有公共公钥 PK、所有验证节点的分片公钥 X_i 及自身的分片私钥 x_i。

3)生成签名

输入消息 M，验证节点对 M 的真实性进行校验，若 M 为真，则用自己的分片私钥 x_i 对 M 进行签名。计算 $m := Hash(M)$，选择随机数 $y \in F_r$，计算 $R := y^{-1} \cdot G$，取 R 横坐标 $r := R \bmod |F_r|$，$s := y(m + x_i r)$，签名为 (r, s)。

4)验证签名

时间轮换公证人组中超过一半的验证节点签名后，使用公共公钥 PK 验证签名，若验证成功，则跨链交易成功实施。输入消息 M，计算 $m := Hash(M)$，校验 $r, s \in F_r$，计算 $R' := (s^{-1}m) \cdot G + (s^{-1}r) \cdot PK$，取 R' 横坐标 $r' := R' \bmod |F_r|$，校验 $r == r'$。

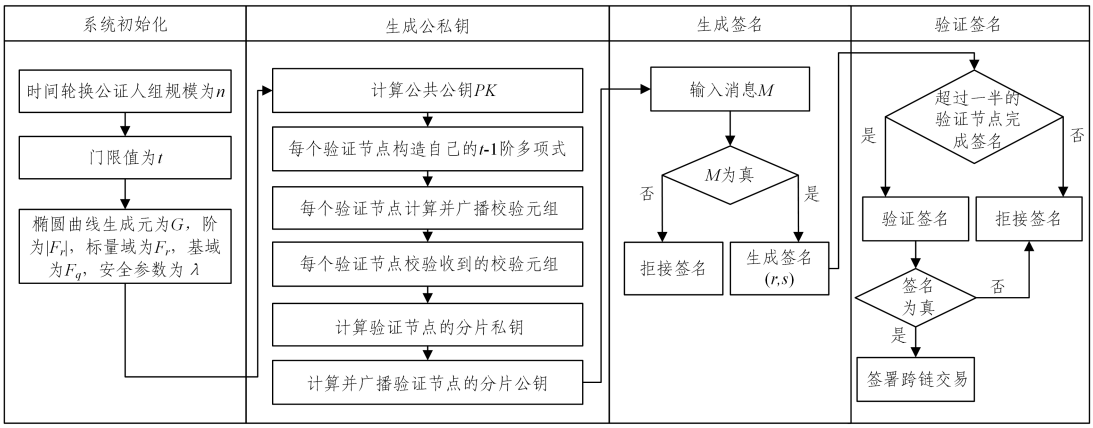

图 4 签名流程

Fig. 4 Signature process

3.3.6 退出时间轮换公证人组

时间轮换公证人组中的验证节点退出方式有两种，分别是正常退出和异常退出。

1)正常退出

当时间轮换公证人组中的验证节点完成跨链交易验证工作且任期时间已至，则此验证节点可正常退出时间轮换公证人组。正常退出的验证节点可拿回之前缴纳的保证金，并获得验证工作的酬劳。

2)异常退出

异常退出分为主动退出和被动退出两种情况。

当时间轮换公证人组中的某个验证节点任期未到，但不想继续充当公证人，则可申请主动退出时间轮换公证人组。主动退出的验证节点不仅不能获得验证工作的酬劳，而且会被扣除一定比例的保证金，用于奖励临时被选中来代替它身份的新验证节点。

当时间轮换公证人组中的某个验证节点违规操作或成为恶意节点，则此验证节点会被动退出时间轮换公证人组，即被时间轮换公证人组清除出去。被动退出的验证节点缴纳的保证金会被没收，不予退还。

对于异常退出的验证节点，需禁止其参加 N 轮时间轮换公证人组的选拔，N 轮过后才可重新计算信用值参与选拔。通过禁选的方式可以进一步降低时间轮换公证人组中验证节点的恶意攻击率。

4 时间轮换公证人组模型分析

4.1 安全分析

时间轮换公证人组的安全性对于跨链交易来说十分重要。本节主要对时间轮换公证人组的去中心化程度、恶意攻击率、黑客攻击、公钥攻击、私钥攻击、合谋攻击进行分析并给予证明。

1)公证人组的去中心化性

传统的公证人机制中心化程度相对较高，若公证人受到攻击，交易资产的安全性就会失去保障，因此提升公证人的去中心化程度对于提升交易资产的安全性十分重要。源链和目标链中的节点需经过可信任集合和候选公证人组的选拔才能进入时间轮换公证人组成为验证节点，且验证节点有任期要求，超过任期的验证节点会被新的高信用值节点代替。与传统的公证人机制相比，时间轮换公证人组的去中心化性程度相对较高，因而安全性较高。

2)验证节点的恶意攻击率

若想成为时间轮换公证人组中的验证节点，需先加入可信任集合，可信任集合中均是经过改进 PageRank 算法审核筛选后存留下的高信任值节点，恶意节点率低，因而恶意攻击率低。

时间轮换公证人组中的验证节点在源链和目标链上均有账户，若来源于源链的验证节点联合作恶，损害目标链的利益，则作恶节点在目标链上的账户利益也会遭受损失，反之亦然。因此，来源于同一条链的验证节点联合作恶损害另一条链利益的概率较低。

若验证节点异常退出时间轮换公证人组，则此节点不能参加 N 次时间轮换公证人组的选拔。通过禁选的方式进一步降低了验证节点恶意攻击率。

时间轮换公证人组中的验证节点均要质押保证金，若验证节点成为恶意节点，则没收该验证节点缴纳的保证金。通过质押保证金的方式，降低了验证节点的恶意攻击率。

3)黑客攻击

多重签名会将参与签名的验证节点和签名地址公开，黑客能够根据公开的信息直接攻击参与签名的验证节点，伪造签名签署跨链交易。时间轮换公证人组模型采用 TSS 方案进行签名工作，参与验证签名的节点信息不可见，私密性高，安全性高。由于验证节点有任期限制，因此黑客在任期内找到验证节点的概率较低。若黑客成功找到验证节点，则需要在该节点任期内成功攻击一半以上的验证节点并获取签名，才能签署非法跨链交易；且在攻击过程中，时间轮换公证人组中的验证节点会随时间变化而变化，因此黑客成功攻击率较低。

4)公钥攻击

公共公钥 $PK=\sum_{i=1}^{n}u_i\cdot G$，分片私钥 $x_i=\sum_{z=1}^{n}(u_z+\sum_{j=1}^{t-1}a_{z,j})\bmod n$，公共私钥 $sk=\sum_{i=1}^{n}(\lambda_i\cdot x_i)$。假设黑客可以根据公共公钥反推出公共私钥，则说明有限域上椭圆曲线离散对数难题被黑客成功解决，这与事实矛盾，因此黑客不能通过公共公钥获取公共私钥。同理，黑客不能通过验证节点的分片公钥获取分片私钥。

5)私钥攻击

假设黑客可以通过公共私钥进行交易签名,则说明在签名方案中涉及公共私钥。但事实上,整个签名方案中没有计算过公共私钥,而是基于分片私钥计算私钥加性份额 w_i,接着生成签名加性份额 sig_i,最后将签名加性份额累加得到完整签名。

分片公钥 $X_i := PK + G \cdot \sum_{z=1}^{n}(\sum_{j=1}^{t-1} a_{z,j})$,公共公钥 $PK = \sum_{i=1}^{n} u_i \cdot G$,分片私钥 $x_i = \sum_{z=1}^{n}(u_z + \sum_{j=1}^{t-1} a_{z,j}) \bmod n$。假设黑客可以获得分片私钥进行非法签名,则说明黑客成功解决了有限域上椭圆曲线离散对数难题,通过广播的分片公钥反推出了分片私钥,这与事实矛盾,因此黑客不能通过分片私钥进行非法签名。

6)合谋攻击

计算 $R := y^{-1} \cdot G$,取 R 横坐标 $r := R \bmod |F_r|$,$s := y(m + x_i r)$,签名为 (r, s)。假设时间轮换公证人组中存在 t 个以上验证节点,通过合谋冒充其他验证节点生成签名,进而签署非法交易。由于合谋验证节点无法获取其他节点的分片私钥,因此不能冒充其他验证节点签名。假设合谋验证节点能够冒充其他验证节点的签名,则说明合谋验证节点成功解决了有限域上椭圆曲线离散对数难题,这与事实矛盾,因此合谋验证节点不能冒充其他验证节点生成签名。

4.2 效率分析

除了安全性,时间轮换公证人组的效率也很重要。时间轮换公证人组的效率体现在验证跨链消息的时间长短上。验证跨链消息的时间与时间轮换公证人组中验证节点的数量、选举效率和跨链交易的签名效率有关,在验证节点数量不变的情况下,选举和签名效率越高,验证跨链消息所需时间越短。本节主要对验证节点选举效率和跨链交易签名效率进行分析,并通过实验验证时间轮换公证人组的效率。

1)验证节点选举效率

若时间轮换公证人组需要选举新的验证节点替代将要退出的验证节点位置,其无需从源链或目标链中重新选举,而是直接从候选公证人组中选取信用值最高的节点代替退出节点的位置,时间轮换公证人组中其余正常工作的验证节点无需被替换。

与替换公证人组中所有节点相比,仅替换退出的验证节点可以提高选举效率。由于验证节点无法连任,因此除了时间轮换公证人组中的验证节点和刚退出的验证节点外,候选公证人组中的节点是信用值最高的一组节点。直接从候选公证人组中选取信用值最高的节点可节省选举时间,提高选举效率。

2)跨链交易签名效率

中心化公证人机制只需单个签名即可验证交易,效率高,但中心化程度相对较高,安全性较低。多重签名公证人机制与中心化公证人机制相比,去中心化程度更高,安全性也更高。但多重签名过程类似于多次单签名,因此多重签名跨链交易签名效率低。时间轮换公证人组模型采用 TSS 方案,从链上来看,产生的签名类似单签。因此与多重签名相比,时间轮换公证人组将签名次数的复杂度从 $O(n)$ 降到 $O(1)$,提升了签名效率。多重签名公证人机制和时间轮换公证人组的签名效率的对比如表 1 所列。除此之外,多重签名公证人机制在签名过程中需要进行多次签名,每次签名都需要消耗 Gas 费。时间轮换公证人组的签名过程类似单签,与多重签名相比,花费的 Gas 费较少。

表 1 签名对比

Table 1 Signature comparison

跨链机制	交易笔数	公证人数	签名次数
多重签名公证人机制	1	n	n
时间轮换公证人组	1	n	1

3)效率实验

本文实验环境基于 Ethereum,在 REMIX 编译器中使用 solidity 语言模拟构建基于时间轮换公证人组模型的多链网络,并在同一环境下模拟构建 Xu 等提出的基于委员会轮换机制跨链模型的多链网络进行对比。

时间轮换公证人组模型的多链网络中包括源链和目标链两条区块链,每条区块链均拥有 6 个节点。基于委员会轮换机制的跨链模型的多链网络与时间轮换公证人组模型的多链网络配置一样。由于委员会轮换机制是在源链和目标链中所有节点中选举委员会,为保证两种方法的选举起点相同,规定多链网络中的所有节点在源链和目标链中均有账户,即时间轮换公证人组模型可以从源链和目标链中所有节点中选举验证节点。为了保证委员会和时间轮换公证人组在验证跨链消息时会发生轮换,设定需被验证的跨链消息数量为 100 条。实验结果如图 5 所示。

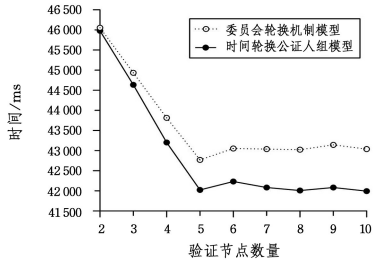

图 5 不同模型的验证时间

Fig. 5 Validation time of different models

由图 5 可知,当验证节点数量相同时,与基于委员会轮换机制的跨链模型相比,时间轮换公证人组模型验证跨链消息所需时间少,效率高。原因包含两方面,一方面,时间轮换公证人组模型只替换失效节点,而基于委员会轮换机制的模型需重组整个委员会;另一方面,时间轮换公证人组模型从候选公证人组中直接选取新的验证节点,而基于委员会轮换机制的模型是重新计算新的信任矩阵,根据新的信任矩阵重选委员会成员。从图 5 中可看出,当验证节点数目为 2 时,验证跨链消息所需时间最长,当验证节点数目为 5 及以上时,验证跨链消息所需时间较短,且基本稳定。因此,验证节点的数目与多链网络中节点数目相关,当多链网络中节点数目很多时,需要的验证节点的数目也较多,以防跨链消息验证时间过长。

结束语 本文提出的时间轮换公证人组模型中的公证人组是由同时拥有源区块链和目标区块链账户的节点经过选举产生的高信用值验证节点组成。公证人组中的验证节点有任期限制,任期已到的失效节点会被新验证节点代替,由于验证节点按任期进行轮换,因此时间轮换公证人组的去中心化

程度较高。时间轮换公证人组模型规定公证人组中的验证节点均要质押保证金，用保证金牵制验证节点的行为规范，可降低验证节点的恶意攻击率。时间轮换公证人组模型规定只有超过一半的验证节点验证签名，才能让跨链交易成功实施，通过提升签名比例，加大黑客攻击难度，提升跨链桥验证环节的安全性。时间轮换公证人组模型采用门限签名方案进行签名工作，加强验证节点信息私密性，提升签名效率，降低签名手续费。将候选公证人组作为时间轮换公证人组中新验证节点的候选组，提升验证节点的选举效率，进而提升跨链消息验证效率。采用时间轮换公证人组模型对跨链交易进行验证，可以更高效地验证跨链交易并保证跨链资产的安全。

跨链过程中资金流经的地方都有被攻击的风险，比如源区块链将未充分检查有效性的交易发布到区块中；验证环节的验证人被控制签署非法交易；目标区块链中黑客通过将keepers的公钥改为自己的公钥来获得非法资产等。本文提出的时间轮换公证人组模型提升了验证环节的安全性，但对于跨链交易来说，源区块链和目标区块链的安全性同样重要，这也是未来需要进一步研究探索的领域。

参 考 文 献

[1] NAKAMOTO S. Bitcoin：A peer-to-peer electronic cash system [EB/OL]. http://bitcoin.org/bitcoin.pdf.

[2] BUTERIN V. A next-generation smart contract and decentralized application platform [EB/OL]. https://github.com/ethereum/wiki/wiki/White-Paper.

[3] SCHWARTZ D, YOUNGS N, BRITTO A. The Ripple protocol consensus algorithm[EB/OL]. https://ripple.com/files/ripple_consensus_whitepaper.pdf.

[4] TIAN Z H, ZHAO J D. Overview of block-chain consensus mechanism for Internet of things [J]. Journal of Computer Applications, 2021, 41(4): 917-929.

[5] YE X H, LIU X Y, WANG B H, et al. Distributed Notary Cross-Chain Model for Consortium Chain [J]. Journal of Applied Sciences, 2022, 40(4): 567-582.

[6] WEI S J, LÜ W L, LI S S. Overview on Typical Security Problems in Public Block-chain Applications [J]. Journal of Software, 2022, 33(1): 324-355.

[7] 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.

[8] RAVI D, RAMACHANDRAN S, VIGN-ESH R, et al. Privacy preserving transparent supply chain management through Hyperledger Fabric [J]. Blockchain: Research and Applications, 2022, 3(2): 100072.

[9] 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.

[10] VO H T, WANG Z Y, KARUNAMOORTHY D, et al. Internet of blockchains: techniques and challenges ahead [C] // Proceedings of the 2018 IEEE International Conference on Internet of Things and Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data. 2018: 1574-1581.

[11] DAI B R, JIANG S M, LI D W, et al. Evaluation Model of Cross-chain Notary Mechanism Based on Improved PageRank Algorithm[J]. Computer Engineering, 2021, 47(2): 26-31.

[12] JIANG C Y, FANG L X, ZHANG N, et al. Cross-chain interaction safety model based on notary groups[J]. Journal of Computer Applications, 2022, 42(11): 3438-3443.

[13] XU Q, ZHAI J H. Research on cross-chain data integration technology based on committee rotation mechanism [J]. Intelligent Computer and Applications, 2023, 13(1): 213-220.

[14] LU A T, ZHAO K, YANG J Y, et al. Research on Cross-chain Technology of Blockchain [J]. Netinfo Security, 2019(8): 83-90.

[15] MENG B, WANG Y B, ZHAO C, et al. Survey on Cross-Chain Protocols of Blockchain [J]. Journal of Frontiers of Computer Science and Technology, 2022, 16(10): 2177-2192.

[16] LI F, LI Z R, ZHAO H. Research on the progress of blockchain cross chain technology[J]. Journal of Software, 2019, 30(6): 1649-1660.

[17] 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.

[18] SHEN C N. Review on cross-chain technology research of blockchains[J]. Chinese Journal on Internet of Things, 2022, 6(4): 183-196.

[19] YU C F, WANG L, ZHOU A H, et al. Method and apparatus for performing multi-party secure computing based on issuing certificate: US2021067347[P]. 2021.

[20] CONSENSYS. BTC Relay's documentation [EB/OL]. https://btcrelay.readthedocs.io/en/la-test/.

[21] POON J, DRYJA T. The bitcoin lightning network: Scalable off-chain instant payments [J/OL]. https://lightning.network/lightning-network-paper.pdf.

[22] WANG Q, LI F J, NI X L, et al. Research on Blockchain Interoperability and Cross-Chain Technology[J]. Journal of Frontiers of Computer Science and Technology, 2023, 17(8): 1749-1775.

[23] SUN Z, ZHU X S, LIU X L, et al. Off-chain consensus scheme of distributed oracles based on threshold signature[J]. Computer Engineering and Design, 2023, 44(1): 37-44.

ZANG Wenyang, born in 1996, master. Her main research interests include blockchain and cross-chain.

LYU Jinlai, born in 1962, master, associate professor. His main research interests include video picture processing and blockchain.

（责任编辑：何杨）