基于跨链技术的跨境海关监管系统研究与实践

吴相豪[1] 戴俊娣[1] 朱文涛[1] 张海涛[1]
WU Xianghao DAI Jundi ZHU Wentao ZHANG Haitao

摘 要 在跨境贸易监管中，传统的数据交换技术在安全性、开放性等方面无法满足海关监管需求。为提高跨境物流监管效率，实现海关监管数据的互联互通，设计一种基于区块链跨链技术的海关监管系统，实现多国异构区块链间跨链物流信息交换及跨境监管。为验证系统的可行性，以多个国家之间的跨境物流监管为例进行实验分析，研究基于中继链跨链技术实现异构链之间跨境物流数据的互联互通，为跨境贸易提供多方共同治理的高安全互联互信系统。结果表明，基于区块链跨链技术的跨境物流海关监管系统在数据共享效率、安全性、系统扩展性和系统运行稳定性等方面表现良好，满足跨境贸易场景下海关监管数据可追溯、去中心化和异构区块链互联互通的应用需求，为跨境贸易“智享联通”提供了一种可行的系统平台。

关键词 区块链；跨链技术；中继链；跨境物流；海关监管

doi：10.3969/j.issn.1672-9528.2024.03.042

0 引言

区块链[1]是运用数字签名、现代密码学、时间戳和智能合约等技术实现的一种分布式基础架构与计算方式。随着区块链概念的提出，各国海关为提高监管效率、降低贸易风险，逐渐将区块链技术应用于海关监管中[2]。借助区块链技术，海关监管将更加全面、真实、便捷。但因各个国家区块链彼此独立、架构各异且互不相通，不利于全球贸易便利化，也与互联互通的国际发展形势不符。

本文设计一种基于区块链跨链技术的海关监管系统平台，其目的是建立一个连接跨境贸易相关国家的异构链的跨链网络，为沿线各国海关提供更安全可靠的跨链服务。为实现更多的区块链系统能够跨链互操作[3]，系统采用符合跨链国际标准的跨链技术。

1 海关区块链应用现状

世界海关组织（WCO）针对区块链在海关领域内的研究报告[4]指出：借助区块链技术，海关能够更广泛、更清晰地了解国际贸易，可以成为一个具有更强大能力的全面边境监管机构。目前，国内外海关领域针对区块链技术的应用已有较多案例和研发项目。

1.1 国内外海关区块链应用现状

国际上，韩国海关实现了基于区块链的电子商务清关平台，美国海关与边境保卫局实现了电子文件的区块链验证。迪拜海关建设基于区块链的跨境电商平台，实现电商交易百分百可见性和可追溯性。

国内，上海海关基于区块链实现了商品溯源应用，厦门海关实现了基于区块链技术的跨境贸易新模式，天津口岸将区块链技术应用于平行进口汽车监管。

1.2 跨链技术的发展

2013 年，Nolan 在 BitcoinTalk 论坛基于比特币系统提出了在数字资产交换场景下进行原子转移的方法[5]，其方法基于哈希锁定技术实现。2019 年 8 月，Li 等人提出了一种基于多重签名的跨链系统 AgentChain[6]。2020 年，跨链协作平台 WeCross 团队开源代码并发布了白皮书，基于哈希锁定机制实现跨链互操作。同年，文献 [7] 提出通用跨链传输协议（Inter-Blockchain Transfer Protocol，IBTP），实现了开源跨链平台 BitXHub，并发布了 BitXHub 白皮书[8]。2023 年，蚂蚁链开源 AntChain Bridge。AntChain Bridge 基于全球首个跨链通用国际标准——IEEE 跨链标准创建，具有全球通用、高安全、极简适配的特性。

1.3 跨境贸易数据共享现状

跨境贸易物流监管的目标是实现贸易的安全、合法和顺畅，与其他国家和地区合作，加强信息交流、数据共享和经验互助，共建开放、透明和有序的跨境贸易物流环境。

对于跨境贸易中多国多信息的共享和互联，目前采用传统的数据交换方式实现，存在中心化结构、安全性保障低、数据一致性难等问题，不能满足跨境贸易中高效监管、便捷通关的趋势目标。

1. 同方威视技术股份有限公司 北京 100084

2 相关技术

跨链技术是指在多个区块链之间建立互操作性和数据共享的技术，解决区块链孤岛问题，提供高效的交互方式。门限秘密共享技术可以增强跨链操作的安全性和合规性，并保护参与方的隐私。

2.1 跨链技术

目前跨链技术分为以下几类。

（1）公证人机制：通过一个公正独立的第三方作为两条链之间的中介，由公证人来协助验证交易。

（2）侧链：依附于主链，是与主链相似的一条规模较小的区块链，能够接收并读取主链交易的资料和数据。

（3）中继链：不依附于任何区块链，是与其他区块链对等、平行的链，通过跨链消息传递协议，连接区块链网络中的其它链。

（4）哈希锁定：使用带有哈希锁定机制的合约进行资产锁定实现质押效果，为不同资产之间的交易提供了信任基础。

（5）分布式私钥控制：运用智能合约，投射原链上的资产到其他不同的链上，同时产生一组控制这些资产的私钥。

上述跨链技术对比分析如表 1 所示。

表 1 跨链技术比对表

对比项	公证人机制 [9]	侧链 [10]/中继链 [11]	哈希锁定 [12]	分布式私钥控制 [13]
原链支持	高	高	低	高
运行效率	高	低	高	低
实现难度	低	高	低	较高
安全性	低	高	较高	较高
适用范围	适用安全性要求不高，但交易效率要求比较高的场景	支持同构和异构链互联互通、实现多条链通道	仅适用于资产兑换	适用安全性要求高，但运行效率无严格要求的场景

当前基于中继链，结合 AES 和 CP-ABE 加密算法实现的跨链医疗数据安全共享方案 [14]，已通过验证并逐步落地。未来跨境贸易互联将是多对多的场景，合理应用中继链将能更好地满足跨境物流监管的需求。

2.2 门限秘密共享

门限秘密共享将信息分割成多个部分，然后将这些部分分发给不同的参与方。只有在达到门限值时，才能重新恢复出完整的信息。

门限秘密 (m, n) 有两个参数：n 和 m。n 表示参与分割秘密信息的参与者数量，m 表示至少几个参与者聚到一起才可以恢复出秘密信息。

秘密分割算法具体运算过程如下。

（1）选择一个随机素数 p，并产生一个随机的 m-1 次多项式，其公式为：

$$f(x) = a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 \bmod p \qquad (1)$$

式中：令 $a_0 = s$。易知，$f(0) = a_0 = s$。注意：$f(x)$ 总是设成 m-1 次。

（2）选择 n 个互不相同的整数 $1 \le x_1, \cdots, x_n \le p$-1。

（3）第 i 个参与者获得 $k_i = f(x_i)$ 作为他的 share，并保密。

（4）销毁 $f(x)$。

秘密重构算法具体运算过程如下。

（1）当有 m 个参与者聚到一起时，他们拿出自己的 share。假设 $k_1, \cdots, k_m$ 是这 m 个 share，分别对应 $x_1, \cdots, x_m$。于是，他们可以如下重构出 $f(x)$，其公式为：

$$f(x) = \sum_{i=1}^{m} \frac{k_i(x-x_1)\ldots(x-x_{i-1})(x-x_{i+1})\ldots(x-x_m)}{(x_i-x_1)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_m)} \bmod p \qquad (2)$$

（2）重构出 $f(x)$ 后，再计算 $f(0)$ 就可以恢复 s。

（3）多于 m 个参与者的情况，以上重构 $f(x)$ 的过程也是适用的。

门限秘密共享在区块链跨链中的应用意义是提供了安全 [15]、去中心化 [16] 的资产跨链转移和多方计算解决方案。它可以增强跨链操作的安全性和合规性，并保护参与方的隐私。

3 跨境物流海关监管系统

基于跨链技术的跨境物流监管系统选择开源的蚂蚁链跨链桥（AntChain Bridge）实现。蚂蚁链跨链桥基于 IEEE P3205 标准的跨链协议 [17]，通过插件化的智能合约部署方式，实现了同构或异构区块链之间的跨链通信和数据传输能力。

3.1 业务场景设计

海关进出境的货物数据主要包括三部分：一是报关数据，二是查验数据，三是物流数据。申报数据、查验数据来源于出口国；物流数据来源于出口国、途经国和目的国，具体业务场景如图 1 所示。

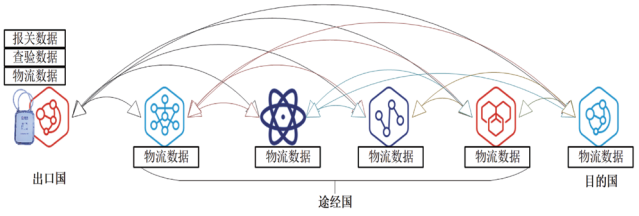

图 1 跨链数据共享业务场景

（1）报关数据同步机制：进出口货物的申报信息以结构化数据为主，附带部分证明材料文件的照片，考虑到链路带宽以及同步效率，可以将结构化申报数据打包到链上存储，并将该区块数据与途经国和目的国同步，完成一次数据交易。

（2）物流数据同步机制：物流数据以结构化数据为主，全部结构化物流数据打包到链上存储，并将该区块数据与途经国和目的国同步，完成一次数据交易。

（3）查验数据同步机制：查验数据主要包括箱号、扫描图像等信息。除扫描图像外，其他都是结构化数据，结构化查验数据打包存储到链上，扫描图像是核心数据，为了避免被篡改和保障数据的真实性，在区块链上保存图像的 Hash 值。通过 Hash 比对，验证图像的真实性，实现快速查验放行。

3.2 系统总体架构设计

系统架构整体由同构 / 异构区块链层、跨链服务层、业务服务层三部分组成，如图 2 所示。通过跨链服务在底层区块链中的协议栈和跨链合约，实现同构或异构区块链之间可信交互，从而构成区块链价值网络，实现链上数据的可信流转，完成丰富的链间互操作。

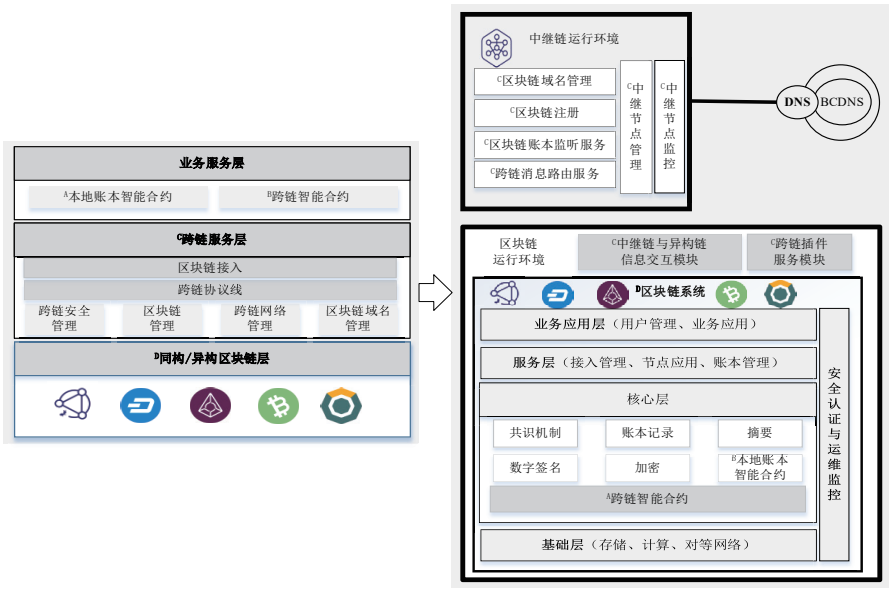

图 2 系统整体功能架构

在 AntChain Bridge 的跨链架构中，中继链网络由多个中继节点组成，通过中继链提供跨链服务。中继链和区块链之间的交互，需要通过区块链桥接组件（blockchain bridge component，BBC）来完成。BBC 是以插件的形式实现的，具体包括链上插件和链下插件两个模块。链上插件是直接部署在异构链上的跨链系统合约，同所有区块链智能合约一样都运行在链上，负责链上跨链消息的可信收发处理；链下插件负责中继和异构链之间的信息交互处理， 是运行在区块链运行环境下的普通 Jar 可执行文件；插件服务模块可以实现对跨链插件的管理，包括部署、启停和运行监控。

在整个跨链交互网络中，为了保障加入的区块链是安全的，申请加入的区块链必须通过域名系统（BCDNS）申请域名，BCDNS 会为接入的区块链颁发域名证书，该域名将会和该链的共识信息唯一绑定，整个跨链网络都可以通过验证域名证书，进而验证该链的合法性。已经在 BCDNS 上注册的区块链，可以将从 BCDNS 获得的域名证书和自签名的区块链的信任锚定（blockchain trust anchor，BTA）提交给中继节点，完成该区块链域名在中继链上的注册。

如图 3 所示，模拟一次跨境物流数据交易流程。（1）数据主体发送给跨链数据交易请求，交易触发应用智能合约，应用智能合约调用跨链智能合约的跨链发送接口，产生特定的跨链事件，发送给中继链上的中继。（2）中继会过滤账本数据中的跨链事件等信号，从事件等数据结构中获取出跨链的消息体， 获取账本提供的存在性证明，连同当前高度验证过的区块头一起交给证明转化组件（PTC）。（3）PTC 完成存在性验证和背书，并给出第三方证明（签名集合），之后将进入跨链消息的中继路由阶段。（4）中继在完成跨链消息和 PTC 背书之后，将解析消息中的接收域名，请求 BCDNS 询问该域名的路由信息，即应该将消息转发给哪个中继节点，如果发送中继本身正在服务这个域名，则直接跳过转发阶段；调用接收中继，转发消息以及证明；接收中继执行 ACL 验证等操作，通过后，接收中继将通过接收链的 BBC 实例，发送交易，提供跨链消息、证明和第三方信任根（third-party blockchain trust anchor，TP-BTA）。

（5）跨链智能合约使用 TP-BTA 验证证明，并解包可认证消息、消息推送协议消息，进而找到接收的账户地址，跨链智能合约调用接收链的应用智能合约完成消息投递。

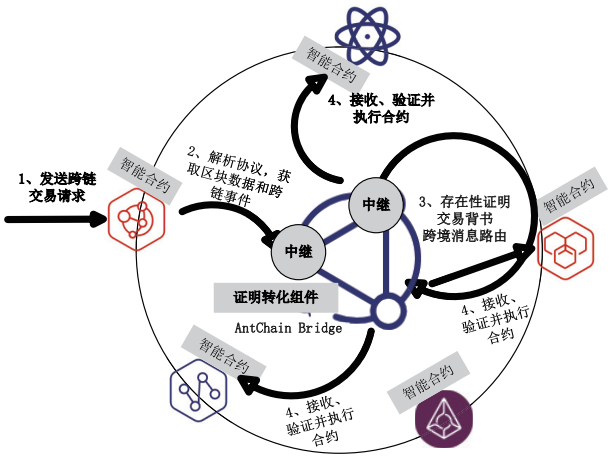

图 3 跨链物流数据交易流程

3.3 信息安全设计

跨链技术本质上是一种将 A 链上的数据安全可信地转移到 B 链，并在 B 链上产生预期效果的一种技术。跨链物流数据交易一定要保证数据的安全性，保障跨链数据的可靠可信且不会泄露。

在利用中继链实现跨链数据传输时，首先参与跨链的各区块链均需申请区块链证书，以便在进行跨链数据传输时，确保源区块链和目标区块链能够相互通过域名证书进行认证，并能够对跨链数据传输的数据进行加密。

成功申请区块链域名证书并完成安装之后，就可以通过中继链实现跨链数据传输。在进行跨链数据传输过程中，可以利用数据加密和签名等方式来保证数据的安全。

中继链在实现跨链的过程中提供了互操作性和扩展性的优势，但同时也会有一些安全性、可靠性和隐私性的挑战。比如，中继链需要获取跨链交易的相关信息和数据以进行验证，这可能涉及用户隐私和数据安全方面的问题，需要在设计时综合考虑各种因素，采取适当措施来解决这些安全性问题。

在采用中继链作为跨链交互的第三方时，引入门限签名（threshold signature scheme，TSS）协议来加强中继链的安全性，以实现在跨链交互过程中，对跨链传输数据的签名和验证，确保中继链的任何单一节点均无法独立完成对跨链数据的签名。

首先，根据中继节点的数量 n，确定参与签名的门限值 m。然后，将私钥拆分成多个部分 K_{priv1}、K_{priv2}、…、K_{privn}，分发给中继节点，并计算出数据验证公钥 K_{pub} 公开发布给所有参与跨链的区块链。密钥生成和分发等初始化工作完成后，就可以在中继链和区块链之间利用门限签名进行数据签名和验证。

4 测试与验证

4.1 实验场景

实验模拟跨境物流海关监管的业务场景，如图 4 所示，出口国的贸易物流数据存储在出口国的区块链 A 中；途经一个或两个途经国，它的贸易物流数据存储在途经国各自的区块链 B 和区块链 B1 中；进口国的贸易物流数据存储在进口国的区块链 C 中。

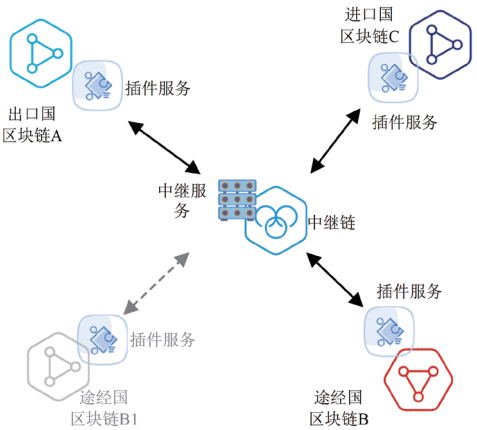

图 4 实验环境部署架构

当货物从出口国进入到途经国时，通过智能合约利用中继链将区块链 A 上的物流数据同步到途经国的区块链 B（或 B1）上；当货物从一个途经国进入另一个途经国时，通过智能合约利用中继链将区块链 B（或 B1）上的物流数据同步到另一个途经国的区块链 B1（或 B）上；当货物从途经国进入到进口国时，通过智能合约利用中继链将区块链 B（或 B1）上的物流数据同步到进口国的区块链 C 上，包括途经国的贸易物流数据。

以跨境货物监管的主体为对象，选择合适的数据类型定义跨境货物数据信息。跨境货物主要对象的结构体包括报关单类、商品类、查验类、物流类结构体。每笔测试用业务数据大约为 5 kB。

4.2 实验环境

实验在 21 个虚拟服务器节点和蚂蚁链 BaaS 服务上进行，所有虚拟服务器节点的配置相同，单个虚拟服务器的配置信息如表 2 所示。

表 2 测试环境配置信息

CPU (vCores)	RAM/GB	Storage/GB	OS
4	32	500	Ubuntu 20.04 LTS

其中，区块链 A 使用 4 个节点，部署 JDChain 集群；区块链 B 和 B1 各使用 4 个节点，部署 Hyperledger Fabric 集群；区块链 C 使用 4 个节点，部署 EOS 集群；每个区块链使用一个节点部署异构链插件服务；中继链使用蚂蚁链 BaaS 服务，共 4 个节点，使用一个节点部署 AntChain Bridge 中继服务。

4.3 实验过程与结果分析

实验将每秒发生多少笔跨链数据同步作为自变量，将中继链每秒能处理多少笔跨链数据同步（TPS）、每笔数据同步的平均延时（latency）作为因变量。实验结果均不考虑数据在各国区块链上的开销。实验通过动态增加途经国的测试方案验证系统的扩展能力和接入难度。

（1）吞吐量测试

在性能测试时，仅接入途经国区块链 B，所有数据都是从出口国经过该途经国，再到进口国。实验通过逐步增大发送需要同步的跨链数据的速率，测试 AntChain Bridge 中继的峰值吞吐量。实验结果如图 5 所示。可以看出，在每笔业务数据约为 5 kB 的情况下，系统的吞吐量峰值约为 9000 tx/sec；从区块链 B 同步数据到区块链 C 的吞吐量略低于从区块链 A 同步数据到区块链 B。

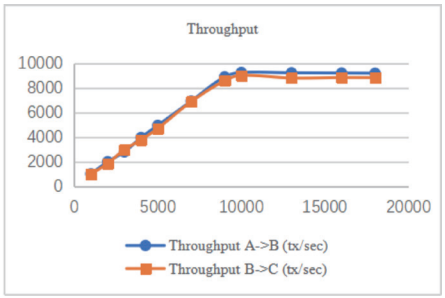

图 5 吞吐量随跨链交易请求速率的变化情况

（2）延迟测试

4 个节点的情况下，中继链处理一笔系统合约需要 100 ms 确认时延；中继服务处理一笔从区块链 A 向区块链 B

的跨链数据同步业务，除去区块链 A 和区块链 B 交易处理时间，平均延迟约为 350 ms；中继服务处理一笔从区块链 B 向区块链 C 的跨链数据同步业务，除去区块链 B 和区块链 C 交易处理时间，平均延迟约为 380 ms。

（3）资源消耗测试

实验过程中使用Perf工具对系统资源消耗情况进行监测，结果表明，在中继链进行跨链数据同步时有一定的网络开销，网络流量与跨链交易量近似成正比；由于在跨链数据同步时需要进行数字签名和数据加解密，插件服务和中继服务会占用一定的 CPU 和内存资源，且中继服务的 CPU 和内存资源消耗大于插件服务，高峰时占总资源的比例不到 50%，对系统性能未造成影响。插件服务和中继服务仅转发消息，不消耗硬盘存储资源，因此对硬盘存储资源的消耗可以忽略。

5 结语

本文设计一种基于跨链技术的跨境物流海关监管系统，为跨境贸易“智享联通”提供了更安全的平台。系统以中继链跨链技术为基础，通过中继链组件实现了一个交易可追溯、安全可靠的去中心化异构区块链互联互通系统。

实验结果表明，该系统可行性高，具有去中心化、可扩展、高可用、易接入等特性，为异构链数据互联互通提供了多方共同治理、高安全、高可信系统。下一步可优化门限秘密共享的算法，同时优化系统部署方式，实现在不同业务场景下图像数据实时交换，提高跨境物流监管数据的安全性与数据互换的高效性。

参考文献：

[1]NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL].(2009-10-06). https://bitcoin.org/bitcoin.pdf.

[2] 李涛，张勇，费立蜀，等．区块链技术在海关现场监管中的应用研究 [J]. 中国口岸科学技术 ,2020(3):23-34.

[3]Institute of Electrical and Electronics Engineers. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries[S/OL]. Piscataway: IEEE, 1990. https://ieeexplore.ieee.org/document/182763

[4]WCO Research Paper No.45 Unveiling the Potentia of Blockchain forCustoms[EB/OL].https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/research/research-paper-series/45_yotaro_okazaki_unveiling_the_potential_of_blockchain_for_customs.pdf?la=en.

[5] NOLAN T. Alt chains and atomic transfers[EB/OL].(2013-05-02). https://bitcointalk.org/index.php?topic=193281.0.

[6]LI D W, LIU J W, TANG Z X, et al. AgentChain: a decentralized cross-chain exchange system[C]//Proceedings of the 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering,Rotorua, Aug 5-8, 2019. Piscataway: IEEE, 2019: 491-498.

[7]WANG H ,HE D ,GAO Y , et al. Research on data verification and exchange of heterogeneous blockchains for electricity application[EB/OL].(2020-07-01)[2023-12-01].https://iopscience.iop.org/article/10.1088/1742-6596/1631/1/012154.

[8] 汪小益，李瑞阳．BitXHub 白皮书 V2.0: 区块链跨链技术平台 [R/OL]. 杭州：趣链科技 ,2021.(2022-07-12)[2023-02-21]. https://upload.hyperchain.cn/BitXHub%E7%99%BD%E7%9A%AE%E4%B9%A6.pdf.

[9] 戴炳荣，姜胜明，李顿伟，等．基于改进 PageRank 算法的跨链公证人机制评价模型 [J]. 计算机工程 ,2021,47(2):26-31.

[10]GAŽI P, KIAYIAS A, ZINDROS D. Proof- of- stake sidechains[C]//Proceedings of the 2019 IEEE Symposium on Security and Privacy. Piscataway:IEEE, 2019:139-156.

[11]FRAUENTHALER P, SIGWART M, SPANRING C, et al.Testimonium: a cost-efficient blockchain relay[EB/OL]. https://arxiv.org/pdf/2002.12837v1.pdf

[12]DAI B R, JIANG S M, ZHU M L, et al.Research and implementation of cross-chain transaction model based on improved hash- locking[C]//Proceedings of the 2nd InternationalConference on Blockchain and Trustworthy Systems.Singapore: Springer,2020:218-230.

[13]SHI L, GUO Z.Baguena: a practical proof of stake protocol with a robust delegation mechanism[J].Chinese journal of electronics,2020,29(5):887-898.

[14] 何全文，林庆新，林晖，等．基于跨链的医疗数据安全共享方案 [J]. 计算机系统应用 ,2023,32(5):97-104.

[15]WANG B, LI J H. A threshold signature scheme without a trusted party[J].Chinese journal of computers, 2003, 26(11): 1581-1584.

[16]ZHANG Y, HOU Z F, HU D H. A dynamic (t,n) threshold signature authentication scheme without a trusty party [J]. Journal of Hefei University of Technology (Natural Science Edition), 2011,34(9):1341-1344.

[17] IEEE 3205—2023 IEEE 区块链互操作性数据认证和通信协议标准 [EB/OL].https://www.antpedia. com/standard/ 1985831060-1. html.

【作者简介】

吴相豪（1977—），通信作者（email：wuxianghao@nuctech.com），男，山东沂水人，硕士，高级工程师，研究方向：区块链、大数据技术应用。

戴俊娣（1977—），女，江苏无锡人，硕士，高级工程师，研究方向：区块链及跨链应用。

朱文涛（1973—），男，湖北武穴人，本科，工程师，研究方向：区块链技术应用。

张海涛（1976—），男，河北衡水人，硕士，工程师，研究方向：智慧口岸建设。

（收稿日期：2023-12-15）