复杂物联网联盟链系统通信机制研究

乔 蕊 [1, 2, 3] 刘敖迪 [2, 3] 陈 迪 [2, 3] 王清贤 [4]

摘 要 联盟链具有公有链固有的安全性, 其许可准入机制允许对网络结点及规模进行控制, 恰好迎合了物联网 (Internet of things, IoT) 向规模化、智能化发展的需要, 成为物联网学术界研究的热点. 然而, 联盟链在一定程度上违背了区块链去中心化价值和信任体系, 产生了多中心化的复杂区块链生态体系, 为使物联网数字资产在不同联盟链间安全、自主、动态流转, 迫切需要对涉及多个联盟链的复杂系统通信机制进行研究. 基于存在多个特权子群的门限数字签名机制建立多联盟链链间合作共识, 利用授权码构造身份证明, 实现链间实体自主授权过程; 构建跨联盟链交易原子提交协议, 确保异步授权状态同步; 提出多级混合可选信任—验证交易共识机制. 实验表明, 上述机制能够在优化系统性能的同时确保系统的安全性.

关键词 物联网, 联盟链, 跨链共识, 群签名, 原子通信

引用格式 乔蕊, 刘敖迪, 陈迪, 王清贤. 复杂物联网联盟链系统通信机制研究. 自动化学报, 2022, **48**(7): 1847−1860

DOI 10.16383/j.aas.c200106

Communication Mechanism of IoT Consortium Chain in Complex Scenarios

QIAO Rui[1, 2, 3] LIU Ao-Di[2, 3] CHEN Di[2, 3] WANG Qing-Xian[4]

Abstract Consortium chain has the inherent security of public chain, and its permission and access mechanism allows institutions to control network nodes and scale, which exactly meets the need of scale and intelligent development of internet of things (IoT), and has become a hotspot in the research of the internet of things. However, the consortium chain violates the decentralized blockchain to some extent, resulting in multi-centralized complex consortium chain ecosystem. In order to make the digital assets of the internet of things safe, autonomous and dynamic transfer between different consortium chains, it is urgent to research on the communication mechanism of IoT consortium chain in complex scenarios. In this paper a method for establishing cooperation consensus among multiple consortium chains based on the threshold digital signature mechanism is proposed. On this basis, a multi-layer hybrid optional trust-verified transaction consensus mechanism is proposed. Then, the authorization code is used to construct an identity certificate, thereby the autonomous authorization between entities is realized. After that, the cross-consortium chain transaction atomic submission protocol is constructed to ensure that the asynchronous authorization status is synchronized, as well as multiple mixed optional trust-verification transaction consensus mechanism is proposed. Experimental results show that the above mechanism optimizes system performance while ensuring system security a lot.

Key words Internet of things (IoT), consortium chain, cross-chain consensus, group signature, atomic communication

Citation Qiao Rui, Liu Ao-Di, Chen Di, Wang Qing-Xian. Communication mechanism of IoT consortium chain in complex scenarios. *Acta Automatica Sinica*, 2022, **48**(7): 1847−1860

物联网 (Internet of things, IoT) 是通过部署具有一定感知、计算、通信、控制、协同和自治特征的基础设施, 获得物理世界的信息, 通过网络实现信息的传输、协同和处理, 从而实现人与物、物与物之间实时全面感知、动态可靠控制和智能信息服务的互联网络[1]. 根据麦肯锡全球研究院 2018 年 11 月发布的报告预测, 全球物联网市场规模将在 2025 年达到 11 万亿美元, 约占全球经济的 11%, 其市场前景将远远超过计算机、互联网与移动通信等[2]. 物联网规模扩张后, 多种物联网应用之间的交互合作更加密切, 为促进行业智能应用服务水平的进一步提升, 设备间的协作和交互呈现爆发式增长, 用户对隐私、安全、定制消费等需求将进一步加剧[3−4], 迫切需要为功能受限的设备提供可扩展的安全性和

收稿日期 2020-03-04 录用日期 2020-08-05
Manuscript received March 4, 2020; accepted August 5, 2020
国家自然科学基金 (61902447), 河南省科技攻关项目 (202102210154), 河南科技智库调研课题 (HNKJZK-2020-04C) 资助
Supported by National Natural Science Foundation of China (61902447), Scientific and Technological Projects of Henan Province (202102210154), and Henan Science and Technology Think Tank Research Project (HNKJZK-2020-04C)
本文责任编委 张道强
Recommended by Associate Editor ZHANG Dao-Qiang
1. 周口师范学院 周口 466001 2. 战略支援部队信息工程大学 郑州 450001 3. 数学工程与先进计算国家重点实验室 郑州 450001 4. 郑州大学网络空间安全学院 郑州 450002
1. Zhoukou Normal University, Zhoukou 466001 2. Strategic Support Force Information Engineering University, Zhengzhou 450001 3. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001 4. School of Cyber Science and Engineering, Zhengzhou University , Zhengzhou 450002

动态自主通信机制. 围绕上述需求, 研究者和物联网企业都做出很多努力. 常见的物联网解决方案依赖于云服务器–客户端架构[5–7], 然而不同利益主体间很难实现完全信任并进行基于机器数据的自主协作交互. 另一种解决方案是将边缘计算作为云架构的补充[8–10], 但边缘设备和云服务器之间的大量数据传输导致底层网络拥塞, 且无法实现不同利益主体间智能设备的自主交互. 联盟链具有公有链固有的安全性, 其许可准入机制允许对网络结点及规模进行控制, 恰好迎合了物联网向规模化、智能化发展的需要, 成为近期物联网研究的热点[11–13].

建立在物联网联盟链数据及操作授权隐私保护、不可篡改和可追溯特性基础上的物联网自主协作, 将大大提升物联网商业价值[14–15]. 典型的物联网联盟链链间协作场景如图 1 所示, 该场景中, 医院、外部停车场、征信机构均采用联盟链存储和管理各自的数据. 患者拟驾车去医院就诊, 可提前使用智能手机等终端输入个人信息进行就诊预约, 并授权医院从征信机构自主获取该患者的信用评估信息. 医院根据该患者信用等级, 授权该患者使用停车场及部分智能医疗监测设备. 患者可在就诊当日自助完成车辆识别、常规检查、病史记录等, 快速准确地建立就诊档案.

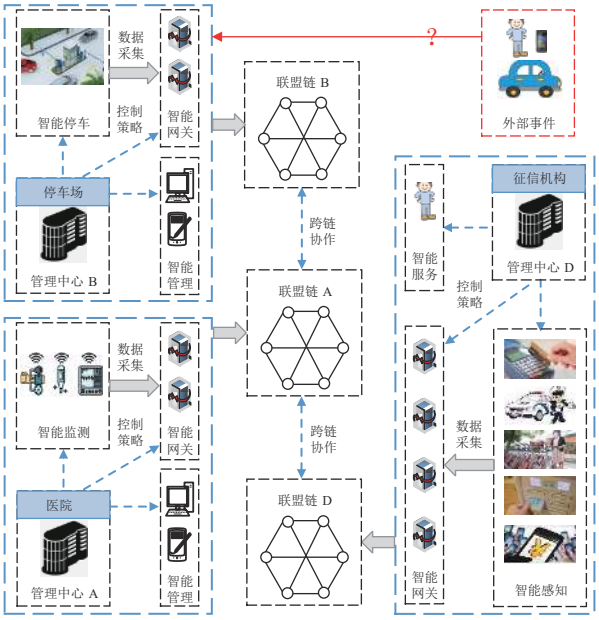


图 1 物联网联盟链链间交互场景图

Fig. 1 Interaction between IoT consortium chains

目前, 学术界和企业界已经在不同的物联网生态及价值体系下, 构建了若干基于联盟链的物联网应用[16–19]. 然而由于联盟链的相互独立性, 产生了多中心化的区块链生态体系, 现存各联盟链之间的数据通信、价值转移等仍面临挑战, 价值孤岛现象逐渐显现[20–22]. 此外, 随着物联网系统规模的扩大, 实际通信场景的复杂化势必造成系统性能和安全性的下降, 对结点跨联盟链通信过程中访问控制机制的可扩展性也提出了新的挑战[23–24].

本文在基于联盟链验证结点列表 VNL (Verification nodes list) 共识和跨链通信机制研究基础上[25–27], 进一步研究复杂场景下物联网联盟链系统自主交互理论模型及算法. 从基于门限数字签名跨链共识 TCCM (Threshold-digital-signature-based cross-chain consensus mechanism) 的可选信任–验证机制、基于 TCCM 自主路由的链间动态授权机制及防止异步授权的跨链原子通信机制三方面对现有物联网通信机制进行改进, 给出一种能够抵御复杂跨联盟链通信系统失效蔓延攻击的异步授权状态同步通信机制, 在优化系统性能的同时确保系统的安全性.

本文的主要贡献如下:

1) 给出结点跨链通信身份可信性路径证明 PPTI (Path proof with trusted identity) 构造规则及基于门限数字签名 TDS (Threshold digital signature) 的递归路径证明生成方法, 将多个联盟链验证结点列表对跨链交易的共识过程建模为存在多个特权子群的 TDS 过程. 在此基础上, 提出能够有效提高系统安全性和可扩展性的基于多级混合共识的可选信任–验证机制.

2) 采用物联网动态数据操作授权多维 DAG (Direct acyclic graph) 存储结构构造授权状态链, 提出构造授权码并运行智能合约交易实现结点间细粒度跨链自主授权方法, 利用存在特权子群的 TDS 共识和非对称密码学原理实现智能合约授权交易的自适应路由.

3) 提出初始化–锁定–解锁三阶段物联网联盟链链间交易原子提交协议, 用于原子地处理跨联盟链交易, 以防止异步授权导致的双重支出攻击和未成功转移的价值被永久锁定, 确保各联盟链之间交易状态的一致性.

本文其余部分安排如下. 第 1 节介绍跨链通信相关研究. 第 2 节分析物联网系统实体自主协作过程, 抽象出复杂场景下物联网联盟链链间通信模型. 第 3 节从联盟链链间合作机制、跨链授权机制、跨链原子通信机制三个方面介绍实现物联网联盟链链间自主动态通信的主要算法改进. 第 4 节通过理论分析及实验部署验证本文机制实现物联网实体跨链通信的安全性和有效性. 第 5 节总结全文.

1 相关工作

将联盟链技术融合应用到物联网领域的挑战之

一是系统可扩展性. 解决不同物联网联盟链实体跨链授权协作及资产交互等通信问题, 是提升物联网联盟链可扩展性的关键. 对于区块链链间通信, 目前已经出现了一些概念验证, 并取得了进展[28], 例如, 以闪电网络为代表的哈希锁定技术, 以 BlockStream 为代表的侧链技术, 以 BTC-Relay 为代表的中继技术, 以 Interledger 为代表的公证人机制, 以 Fusion 为代表的分布式私钥控制技术等. 跨链技术除了沿用早期类质押的思想外, 还提出了区块链结点角色分工、状态通道、信任传递等新的思想[20, 29−33].

早期的跨链技术主要关注资产转移[34−40], 比较著名的有哈希锁定和侧链技术. 哈希锁定技术主要思路是, 为实现用户间小额支付通道, 用户需提前锁定自己的部分款项, 涉及该部分款项的交易在链下进行, 款项的最终分配方案确定后再上传至主链[34−35]. 侧链是以原生数字资产为基础, 和其他账本资产在多个区块链间转移的链间通信技术, 是为解决主链扩展问题而提出的扩容技术[36−37]. 比较著名的比特币侧链有 BlockStream[36] 和 RootStock[38] 的元素链, 非比特币侧链有 Lisk[39] 和国内的 Asch[40] 等.

现有研究更多关注的是链状态的转移[41−45]. 以太坊通过建立在以太坊网络协议之上的多个分片来实现链间通信, 通过一种称为超二次分片的方法指数级地提高网络吞吐量[41], 然而现有分片技术需要几次甚至多次的硬分叉才能完成, 这给现有应用和用户带来很多不便. Ripple 开发的 Interledger 协议[42]通过第三方 “连接器”或 “验证者”进行链间资产交互, 该协议采用密码算法为参与的多条链和连接器创建资金托管, 各链无需信任连接器, 当所有参与方对交易资产量达成共识时, 便可进行资产交互, 只有参与资产交互的区块链系统才可以跟踪交易. Pointnity Network[43] 为解决单一区块链在实际应用场景中无法解决复杂问题, 以及在性能上相对于传统中心化系统所呈现的瓶颈, 提出 “恩特链”区块链跨链网络. Polkadot[44] 采用多链融合的设计模式, 将其他链都视为平行链, 通过中继链 (Relay-chain) 将平行链上的代币转入具有多重签名控制的母链地址中, 对其进行暂时锁定, 在中继链上的交易结果将由签名人共同投票决定是否有效, 从而实现跨链通信. Fusion[45] 将各种加密资产通过分布式私钥生成与控制技术映射到公有链上, 多种被映射加密资产可以在其公有链上进行自由交互.

随着资产上链以及链间通信需求的加剧, 有研究开始探寻基于智能合约的去中心化跨链资产管理方法[46−47]. 以太坊平台提供了图灵完备的智能合约运行环境, 目前已拥有超过 5700 万个账户[48]. ERC20 为以太坊区块链上的资产交易建立了标准合约 ABI (Application binary interface), 共享合约界面, 简化与外部合约的集成, 已成为多类数字资产交易的事实标准[49]. 在以太坊智能合约研究基础上[46], Warren 等[50] 提出了旨在作为开放标准和通用构建块的基于 ERC20 的简明点对点资产交易协议, 通过在开源以太坊智能合约之上开发用于资产交互的分布式应用程序 (Decentralized application, DAPP) 实现资产交易, 并对最终成交交易收取交易费用. 与上述研究不同, Aeternity[51] 构建了高度可扩展的区块链架构及基于预言机 (Oracle) 验证模型的共识机制.

综上所述, 现有区块链跨链通信方面的研究, 引入了资产映射和资产交易概念模型重构区块链价值交换网络. 尽管经过近几年的快速发展, 仍存在一些不足: 1) 主要通过抵押方式保证资产交互的原子性, 处理一般数字资产上链及资产交互事务的实现逻辑较为复杂, 应用场景受限; 2) 抵押方式下, 通过智能合约实现的跨链协同操作, 为保证区块链上一般资产交互事务的原子性, 需在等待一条链返回处理结果的过程中, 将智能合约的状态封存, 从而导致在等待的过程中, 该智能合约无法执行其他请求, 由此带来效率低下、功能缺失等问题, 无法满足物联网商业应用.

2 通信模型

系统中存在资产所有者、发布者、访问者和交易验证者 4 类角色. 本文对通信模型做如下假设:

1) 连接至不同系统的感知设备始终在线; 为了达到一定程度的对等通信, 将感知数据发送至网关, 由网关作为发布者发布感知数据; 实体和资产间关系采用一对多范式, 拥有资产所有权的实体可随时监控系统设备及数据, 对其进行操作并对其他实体进行除所有权外的自治授权; 被授权实体可以访问者身份进行特定操作.

2) 通过联盟链机构审核机制为验证者建立的身份足以抵御 Sybil 攻击.

3) 验证者之间的通信通道是同步的, 即如果某验证者广播了一条消息, 则所有验证者都会在已知的最大通信时延 Δ 内接收到该消息.

复杂跨联盟链系统链间通信模型如图 2 所示. 通信模型中, 有 n 个来自各联盟链的验证者参与交易处理并确保系统状态的一致性, 机构为各联盟链 C_X 中的每个验证者 i 都生成一个公、私钥对 ($C_{X_i.PK}$, $C_{X_i.SK}$), 通过 $C_{X_i.PK}$ 唯一标识验证者 i. 复杂通信情况下, 系统中的一次请求需要由若干个交易协作完成, 如该模型联盟机构 B 中某结点 C_{B_j} 需获得另

两联盟机构 A 和 D 中结点 C_{A_i}、C_{D_k} 协作才能继续执行当前任务. 图 2 (a) 中, 圆形结点为各联盟机构内部参与系统运行的活动实体, 其中, 灰色结点为普通结点, 仅参与交易的生成和中继; 条纹结点为机构预选的验证结点, 除了具备普通结点功能, 还可以对交易进行验证; 黑色结点为某次链间协作涉及到的结点; 有向箭头尾部结点为交易发起结点, 箭头指向结点为交易响应结点. 联盟机构 A, B, D 验证结点总数分别为 n_A, n_B, n_D, 由机构设定联盟链验证结点门限值分别为 t_A, t_B, t_D, 各联盟链验证结点集中实际通过当前验证的结点 (图 2 (b) 中环形结点) 数目分别为 t'_A, t'_B, t'_D. 当实际通过验证结点数目满足群签名机制门限要求时, $C_{A_i}(C_{D_k})$ 响应来自 C_{B_j} 的请求.

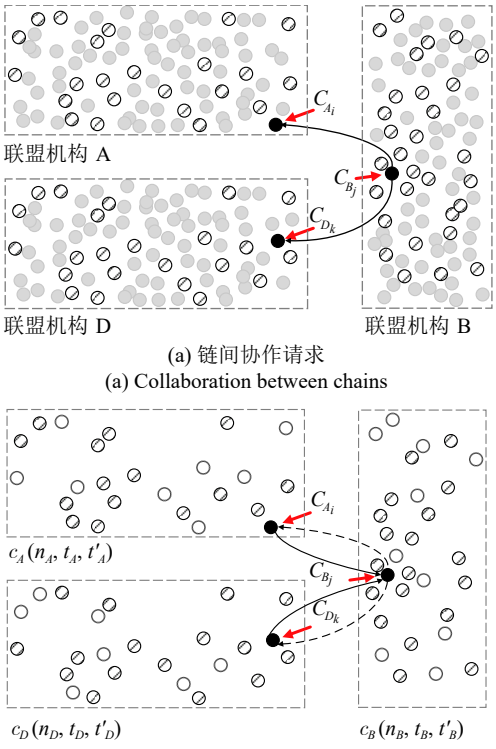


图 2 联盟链链间通信模型

Fig. 2 Consortium cross-chain communication model

本文通过构建基于群门限数字签名的跨链合作机制, 降低异构物联网联盟链数字资产跨链交互的复杂度; 利用存在特权子群的门限数字签名共识算法和非对称密码学原理, 实现对智能合约授权交易的自适应路由, 进而实现结点间跨链无偿–主动授权, 简化验证流程, 提高验证效率; 给出跨链原子通信协议, 以原子方式提交或终止由若干个交易协作完成的跨链请求, 确保跨链通信期间单个联盟链正确、连续处理交易的鲁棒性, 有效抵御失效蔓延攻击.

3 算法设计

复杂情况下跨联盟链通信机制主要包括跨链合作、授权机制、跨链原子通信三部分. 若交易处理的某阶段未通过, 则忽略该交易, 本节仅分析交易处理各阶段均通过的情况.

定义 1. 建立合作关系的 m 个联盟链 C_1, C_2, $\cdots$, C_m 验证结点列表集合记为群 $\mathcal{C}$, 各联盟链验证结点列表记为群 $\mathcal{C}$ 中 m 个互不相交的特权子群 $\mathcal{C}_1$, $\mathcal{C}_2$, $\cdots$, $\mathcal{C}_m$, 存在多个特权子群的门限数字签名共识表示为:

$$\mathcal{C}=\{\mathcal{C}_1 \| \mathcal{C}_2 \| \cdots \| \mathcal{C}_m,\ \mathcal{C}_i \cap \mathcal{C}_j = \emptyset\},\quad 1 \le i,\ j \le m \tag{1}$$

$$|\mathcal{C}_i| = n_i,\quad n_i > 0 \tag{2}$$

$$\sum_{i=1}^{m} n_i = n,\quad m \ge 1 \tag{3}$$

$$E_{SK_{\mathcal{C}_i}}(TX,\ t_i,\ n_i) = \begin{cases} \text{True}, & \text{if } n_i \ge t'_i \ge t_i \\ \text{False}, & \text{otherwise} \end{cases} \tag{4}$$

$$E_{SK_{\mathcal{C}}}(TX,\ t_1,\ n_1; \cdots;\ t_m,\ n_m;\ t,\ n) = \begin{cases} \text{True}, & \text{if } n_i \ge t'_i \ge t_i \ \&\ \sum_{i=1}^{m} t_i \ge t \\ \text{False}, & \text{otherwise} \end{cases} \tag{5}$$

上述定义中, 子群 $\mathcal{C}_i$ 为联盟链 C_i 中验证结点集合, n_i 表示子群 $\mathcal{C}_i$ 验证结点列表中的结点个数, t_i 表示子群 $\mathcal{C}_i$ 的 n_i 个验证结点通过某次验证的最少结点数目, t'_i 表示 n_i 个验证结点中实际通过某次验证的结点数目, t 表示群 $\mathcal{C}$ 的 n 个验证结点通过某次验证的最少结点数目. 式 (1) 限定联盟链间合作关系, 式 (2)、式 (3) 表示联盟链验证结点集规模, 式 (4) 验证联盟链内部基于验证结点列表的 TDS 共识, 式 (5) 验证基于验证结点列表的 TCCM 共识.

3.1 链间合作机制

由联盟机构决定系统对公众的开放程度, 采用椭圆曲线密码算法为联盟机构及实体生成各自的公、私钥对 (PK, SK), 对实体身份进行分类和标识, 构造实体身份证明. 下面介绍为实现不同联盟链实体间自主协作, 构造跨链结点通信路径证明和联盟链链间合作共识证明的方法.

3.1.1 路径证明构造规则

定义 2. $sig(m, X)$ 表示 X 的私钥对消息 m $(m \ne \emptyset)$ 的签名, 三元组 $(m,\ \mathcal{P},\ \sigma)$ 表示交易路径证

明, $\mathcal{P}(TX)=\{u_0,\cdots,\ u_k\}$ 为交易 TX 从请求发起结点 u_0 到最近响应结点 u_k 的有向连通路径, $\sigma=sig(\cdots sig(m,\ u_0),\cdots,u_k)$ 为从 u_0 到 u_k 的路径签名. 若 u_k 为中继响应结点, 从 u_0 到 u_k 的路径证明称为当前路径证明; 若 u_k 为最终响应结点, 从 u_0 到 u_k 的路径证明称为全路径证明.

对 P2P 通信方式下可信传播路径进行简化, 得到路径证明构造规则如下:

规则 1 (聚合规则). 在 PPTI 路径证明拓扑链路上, 将验证结点子群抽象为有向路径证明中的一个结点, 相应地将合法的门限子群签名作为路径签名中的一个签名;

规则 2 (等价规则). 将联盟链内部结点经链内其他结点中继至验证结点子群的 PPTI 路径证明简化为由该结点至验证结点子群的单跳路径证明;

规则 3 (中继规则). 不同联盟链结点间跨链通信 PPTI 路径证明仅包含验证结点子群作为中继结点;

规则 4 (响应规则). PPTI 路径证明中普通结点间的单跳路径表示基于请求发起结点价值转移密钥 s 的盲响应.

由聚合规则, 将验证结点子群 $\mathcal{C}_X$ 抽象为有向 PPTI 路径证明中的一个结点; 由等价规则, 将结点 C_{A_k} 经链内其他结点中继至验证结点子群 $\mathcal{C}_A$ 的 PPTI 路径证明简化为由结点 C_{A_k} 至 $\mathcal{C}_A$ 的单跳路径证明; 由中继规则, $\exists C_{B_j}\in C_B,\ C_{A_i}\in C_A,\ C_A\cap C_B=\emptyset,\ C_{B_j}$ 至 C_{A_i} 的跨链路径证明仅包含通信链路上验证结点子群 $\{\mathcal{C}_B,\cdots,\mathcal{C}_X,\cdots,\mathcal{C}_A\}$ 作为中继结点; 由响应规则, 路径证明链路存在回路, 且任意两普通结点间的 PPTI 路径证明为经过若干验证结点子群中继的多跳路径证明, 两普通结点间的单跳路径为响应结点基于请求结点和响应结点间 PPTI 路径证明对请求结点发出价值转移密钥 s 的单跳响应.

由定义 2, 得到基于 TDS 的递归路径证明生成公式:

$$\begin{aligned}&u_0\xrightarrow{TX_1}u_1:TX_1=m\left\|E_{SK_{u_0}}(m)\right.,\\&u_i\xrightarrow{TX_i}\mathcal{C}_i:TX_{i+1}=m\left\|E_{SK_{\mathcal{C}_i}}(TX_i,\ t_i,\ n_i),\ i>0\right.\end{aligned}\tag{6}$$

其中, 参数 $t_i,\ n_i$ 为可选项, 用于门限签名.

$\forall C_{B_j}\in C_B,\ C_{A_i}\in C_A,\ C_A\cap C_B=\emptyset,\ C_{B_j}$ 以明文方式构造对另一联盟链结点 C_{A_i} 的交互请求 m_{B_j}, 根据路径证明构造规则 2 和生成式 (6) 依次构造 C_{B_j} 至 $\mathcal{C}_B$、$\mathcal{C}_B$ 至 $\mathcal{C}_A$、$\mathcal{C}_A$ 至 C_{A_i} 的 PPTI 路径证明.

3.1.2　基于 TCCM 的合作共识

通信模型中, 群 $\mathcal{C}$ 内存在三个特权子群, 链间路径证明群签名协议标记为 $(t_A,\ n_A;\ t_B,\ n_B;\ t_D,\ n_D;\ t,\ n)$. 为得到 C_{A_i}、C_{D_k} 授权, 除 PPTI 路径证明外, C_{B_j} 还需要向系统提供联盟链链间合作共识路径证明. 基于特权子群的联盟链链间合作共识路径证明构造具体包括群秘钥生成与共享、门限子群签名生成及路径证明更新三部分, 最后由响应结点所在联盟链验证结点子群对路径证明中各门限子群签名进行合成.

由秘钥颁发机构选取安全素数 u、v, 且满足 $v\,|\,(u-1)$; 在有限域 Z_v 上秘密选取 4 个多项式 $f(x)$, $g_A(x),\ g_B(x),\ g_D(x)$, 次数依次为 $(t-1),\ (t_A-1),\ (t_B-1),\ (t_D-1)$. 选取有限域 Z_v 的本原元 α, 公开 $(u,\ v,\ \alpha)$ 和 $x_p,\ y_{A_i},\ y_{B_j},\ y_{D_k}\in {}_RZ_v$; $p=1,\ 2,\cdots,\ n$; $i=1,\ 2,\cdots,\ n_A$; $j=1,\ 2,\cdots,\ n_B$; $k=1,\ 2,\cdots,\ n_D$. 由秘钥颁发机构按照式 (7) 随机产生群私钥, 按照式 (8) 计算群公钥, 群私钥采用基于 Shamir 的秘密共享算法进行分发.

$$SK_{\mathcal{C}}=(f(0)+g_A(0)+g_B(0)+g_D(0))\bmod v\tag{7}$$

$$PK_{\mathcal{C}}=\alpha^{(f(0)+g_A(0)+g_B(0)+g_D(0))\bmod v}\bmod u\tag{8}$$

基于秘密共享算法为特权结点 $\mathcal{C}_q$ 秘密分配群私钥片段 $f(x_q),\ g_A(y_{A_i}),\ g_B(y_{B_j}),\ g_D(y_{D_k})$, 按照式 (9) 计算其公钥并公开.

$$PK_{\mathcal{C}_p}=\alpha^{\lambda_p f(x_p)+\mu_p\sum\limits_X g_X\left(y_{X_{p_i}}\right)}\bmod u,\quad X\in\{A,\ B,\ D\}\tag{9}$$

由式 (2), 子群 $\mathcal{C}_X$ 验证结点个数为 $|\mathcal{C}_X|=n_X$, $(n_X>0,\ X\in\{A,\ B,\ D\})$, 子群 $\mathcal{C}_X$ 的 n_X 个验证结点中通过某次验证的门限结点数目为 t_X. 被签署的交易为 TX. 对于每个 $t_i\in\{t_X\}$, 秘密随机选取 $\mathcal{K}_p\in Z_u^*$, 由式 (10) 计算公钥片段 r_{X_p}, 子群 $\mathcal{C}_i$ 内各验证结点由式 (11) 计算子群公钥 r_X, 由式 (12) 计算单个验证结点私钥片段 s_{X_p}.

$$r_{X_p}=\alpha^{\mathcal{K}_p}\bmod u,\ \mathcal{K}_p\in Z_u^*\tag{10}$$

$$r_X=\prod_{p=1}^{t_X}r_{X_p}\bmod u\tag{11}$$

$$\begin{aligned}s_{X_p}=&(f(x_p)\lambda_p h(TX)+\sum_X g_X(y_{X_{p_i}})\mu_p h(TX)-\\&\mathcal{K}_p r_X)\bmod\ v,\quad X\in\{A,\ B,\ D\}\end{aligned}\tag{12}$$

其中, λ_p、μ_p 是 Shamir 秘密共享算法中公开可计算的拉格朗日系数, $h(x)$ 是安全的哈希函数.

群 $\mathcal{C}$ 内结点由式 (13) 验证子群内单个验证结

点签名 s_{X_p} 的合法性.

$$\alpha^{s_{X_p} r_p{}^{rX}} = PK_{\mathcal{C}_p}{}^{h(TX)},\ X \in \{A,\ B,\ D\} \tag{13}$$

若式 (13) 成立, 验证结点子群接受子群内该单个验证结点签名, 当 $|s_{X_p}| \geq t_X$ 时, 由式 (14) 计算 s_X. 图 2 中, 由验证结点子群 $\mathcal{C}_B$, $\mathcal{C}_D$ 按照上述方法分别输出对交易的子群 TDS (r_B, s_B), (r_D, s_D), 类似地, 由响应结点 C_{A_i} (或 C_{D_k}) 所在联盟链验证结点子群 $\mathcal{C}_A$ (或 $\mathcal{C}_D$) 按照式 (15) 生成子群合成签名 $(r_{\mathcal{C}}, s_{\mathcal{C}})$.

$$s_X = (s_{X_1} + s_{X_2} + \cdots + s_{X_t}) \bmod v,\ X \in \{A,\ B,\ D\} \tag{14}$$

$$\begin{cases} s_{\mathcal{C}} = (s_{A_1} + s_{A_2} + \cdots + s_{A_{t'_A}} + \\ \quad s_{B_1} + s_{B_2} + \cdots + s_{B_{t'_B}} + s_{D_1} + s_{D_2} + \cdots + \\ \quad s_{D_{t'_D}}) \bmod v, \\ (n_A + n_B + n_D) \geq (t'_A + t'_B + t'_D) \geq t, \\ \quad t'_A \geq t_A,\quad t'_B \geq t_B,\quad t'_D \geq t_D \\ r_{\mathcal{C}} = \prod\limits_X r_X \bmod u \end{cases} \tag{15}$$

子群签名合成后, $\mathcal{C}_A$ 按照式 (16) 将对交易 $TX_{B_j.\text{request}}$ 的群签名与 m_{B_j} 一起写入智能合约交易 $TX'_{B_j.\text{request}}$, 更新交易路径证明.

$$\mathcal{C}_A \xrightarrow{TX'_{B_j.\text{request}}} \mathcal{C}_{A_i} : TX'_{B_j.\text{request}} = m_{B_j} \left\| E_{SK_{\mathcal{C}_A}}(TX_{B_j.\text{request}},\ t_A, n_A; t_B, n_B;\ t_D,\ n_D; t,\ n) \right. \tag{16}$$

3.1.3 共识优化

为提高系统安全性, 通常将系统划分为数量少、规模大的联盟链, 而大规模的联盟链又带来交易共识延迟较长的问题. 为解决此问题, 本文根据交易涉及的实体范围, 将交易划分为不同的类型, 采取不同的 TDS 共识方式, 下面给出交易类型的判别式.

$$\begin{aligned} &\exists u_i \in \mathcal{P}(TX) \cup u_i \in C_X, \\ &\quad \forall u_j \in \mathcal{P}(TX) \rightarrow u_j \in C_X\ (j \neq i) \end{aligned} \tag{17}$$

若式 (17) 成立, 该交易为非跨链交易, 否则, 为跨链交易. 系统根据该判别式自动识别跨链与非跨链交易. 基于多级混合共识的信任–验证机制对交易进行验证, 共识架构如图 3 所示.

对于非跨链低价值交易, 由链内验证结点按照式 (18) 对其进行快速共识 (第一级共识).

$$D_{PK_{\mathcal{C}_X}}\left(E_{SK_{\mathcal{C}_X}}(TX,\ t_X,\ n_X)\right) = \begin{cases} TX, & X \in \{A, B, \cdots\} \\ \text{other} \end{cases} \tag{18}$$

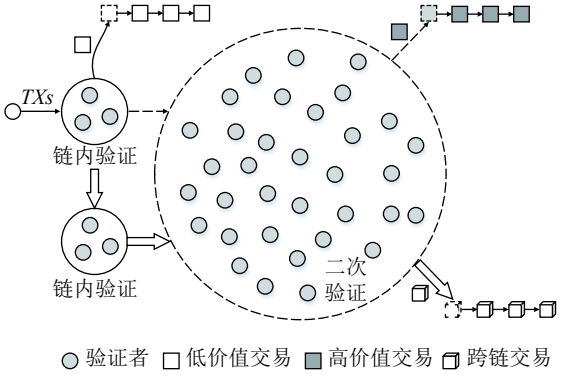


图 3 基于多级混合共识的信任–验证机制

Fig. 3 Multi-consensus based trust-verification mechanism

用户可以选择接受快速共识结果并获得实时的处理效率, 然而, 这并不意味着对系统低价值交易处理完毕. 为保证系统长期运行的安全性, 系统在用户接受快速共识结果后仍需要对低价值交易数据区块进行第二级共识, 当第二级验证结点共识结果与第一级不一致时, 机构将对第一级共识列表中签署了非法区块的验证结点进行识别并追究责任. 一方面, 第二级共识完成时间距离用户接受第一级快速共识的时间并不会太久, 可以较快甄别虚假共识并尽可能挽回损失; 另一方面, 理性参与结点的目标是最大化自己的收益函数, 对于低价值交易, 机构通过引入惩罚机制, 对恶意验证结点采取剔除出 VNL 或其他形式惩罚, 降低结点作恶的可能性. 详细的惩罚机制本文不做讨论.

对于非跨链交易中的高价值交易, 采用多级混合共识中的两级验证机制, 由交易发送者所在联盟链内 VNL 构成第一级共识列表, 根据群签名门限值随机生成来自不同联盟链 VNL 的第二级共识列表, 按照式 (19) 对其进行共识.

对于跨链交易, 采用上述基于存在特权子群 TDS 机制的多级混合共识方式, 根据机构为各结点所在联盟链设定的共识门限值对接收或发出的交易进行链内共识, 由交易的最终响应结点所在联盟链验证结点子群使用群密钥对路径证明中各子群 TDS 进行合成, 按照式 (20) 对其进行共识.

本文提出的多级混合可选信任–验证共识机制通过将交易区分处理, 充分利用链内共识速度较快, 有利于提高系统吞吐量, 第二阶段共识 (跨链) 过程较慢, 但可获得更高安全性的处理特性, 可在不牺牲系统吞吐量和安全性的情况下, 实现低价值交易的实时确认, 同时保障跨链交易和高价值交易的安全性. 因此, 上述机制在微观上最大程度地提高了系统验证资源利用率, 宏观上提升了链内验证和二

次验证并发执行的程度, 从而提升了系统共识效率.

$$\begin{cases} D_{PK_{C_X}}\left(E_{SK_{C_X}}\left(TX,\ t_X,\ n_X\right)\right) = \\ \qquad \begin{cases} TX, & X \in \{A,\ B, \cdots\} \\ \text{other} \end{cases} \\ D_{PK_C}\left(E_{SK_C}\left(TX,\ t_X,\ n_X; \cdots;\ t,\ n\right)\right) = \\ \qquad \begin{cases} TX \\ \text{other} \end{cases} \end{cases} \tag{19}$$

$$\begin{cases} D_{PK_{C_X}}\left(E_{SK_{C_X}}\left(TX,\ t_X,\ n_X\right)\right) = \\ \qquad \begin{cases} TX, & X \in \{A,\ B, \cdots\} \\ \text{other} \end{cases} \\ D_{PK_{C_{X'}}}\left(E_{SK_{C_{X'}}}\left(TX,\ t_{X'},\ n_{X'}\right)\right) = \\ \qquad \begin{cases} TX, & X' \in \{A,\ B, \cdots\} \\ \text{other} \end{cases} \\ D_{PK_C}\left(E_{SK_C}\left(TX,\ t_X,\ n_X; t_{X'},\ n_{X'}; \cdots;\ t,\ n\right)\right) = \\ \qquad \begin{cases} TX \\ \text{other} \end{cases} \end{cases} \tag{20}$$

3.2　基于 TCCM 的无偿−主动授权机制

通过对物联网系统运行逻辑进行分析, 本文对物联网结点间授权协作行为进行细粒度划分, 如图 4 所示, 物联网结点间协作除了存在有偿−请求 (跨链) 授权情况, 在复杂场景下, 还存在无偿−主动 (跨链) 授权情况.

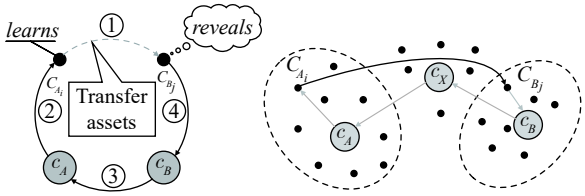


图 4　授权协作的细粒度划分

Fig. 4　Fine-grained division for authorization collaboration

有偿−请求授权是指请求者通过提供授权请求、可信身份证明等, 并在智能合约中托管一定数额承诺转移的资产, 获得目标响应者授权的方式, 如图 4 (a) 所示. 文献 [27] 通过部署基于 VTM (Value transfer mechanism) 机制的智能合约实现了结点间有偿−请求授权. 无偿−主动授权是指由于结点间协作需要, 拥有某项权限的结点需要主动授权给目标结点的情况, 如图 4 (b) 所示, 例如, 联盟链 C_A 中结点 C_{A_i} 需要向联盟链 C_B 中结点 C_{B_j} 授权, 并与 C_{B_j} 一起完成某项任务. 在上述无偿−主动授权过程中, 结点 C_{B_j} 需向结点 C_{A_i} 自主提供可信身份证明 (图 4 (b) 中灰色箭头), C_{A_i} 验证通过后, 才会对 C_{B_j} 进行授权 (图 4 (b) 中黑色箭头). 显然, 无偿−主动授权过程由于缺乏价值激励无法通过 VTM 机制实现. 本节介绍利用存在特权子群的 TDS 共识算法和非对称密码学原理实现对智能合约授权交易自适应路由, 进而实现结点间跨链无偿−主动授权的方法.

为了使不存在依赖关系的交易在异构联盟链中并发处理, 采用文献 [25] 提出的物联网动态数据操作授权多维 DAG 存储结构构造授权状态链, 以维护所有公开授权记录、投票表决表及由实体构成的成员表. 一般情况下, 两个相邻的授权状态区块的 DAG 结构的大部分应该是相同的, 因此, 可以利用指针 (即子树哈希) 方便地实现对已经获得授权的引用, 利用授权码插入和删除结点更新授权链, 授权码定义如下.

定义 3. 授权码 (Authorization code, Acode) 由授权交易的授权方生成, 包括授权方机构公钥、使能标志、授权类型及授权方公钥 4 个部分, 用于提供授权证明、进行授权验证.

通信模型中, 为得到 C_{A_i}、C_{D_k} 授权, 除 PPTI 路径证明外, C_{B_j} 还需要向系统提供联盟链链间合作共识证明. 由于响应结点对请求结点的授权过程具有相似性, 这里仅考虑 C_{A_i} 对 C_{B_j} 的授权过程. C_{A_i} 对式 (16) 中交易 $TX'_{B_j.\text{request}}$ 进行验证, 通过后, 构造包含身份证明 $C_{A_i.\text{Proof}}$ 及对资产 $\xi_{C_{A_i}}$ 授权类型的授权码.

图 5 给出了结点 C_{A_i} 构造授权码, 运行智能合约交易, 实现对结点 C_{B_j} 自主授权的过程 (不包括所有权). C_{A_i} 提供在授权状态链上拥有资产 $\xi_{C_{A_i}}$ 所有权的最新证明, 置授权码中访问控制策略使能标志, 并调用随机函数产生随机数 $nonce$, 用于计数及区分不同的授权; C_{A_i} 用自己的私钥 $C_{A_i.SK}$ (为方便表述, 本文也记作 $SK_{C_{A_i}}$) 对授权码及随机数加密, 得到密文 m_1, 用 C_{B_j} 的公钥 $C_{B_j.PK}$ 对密文 m_1 和 C_{A_i} 的公钥 $C_{A_i.PK}$ 加密, 得到密文 m_2, 用群公钥 $\mathcal{C}_{PK}$ 对 m_2 加密得到 m_3, 然后将 m_3、机构子群验证证明 $\mathcal{C}_{A.\text{Proof}}$ 等作为交易 TX_{m_3} 在物联网联盟链系统网络广播.

被授权结点 C_{B_j} 所在联盟链接收到交易 TX'_{m_3}

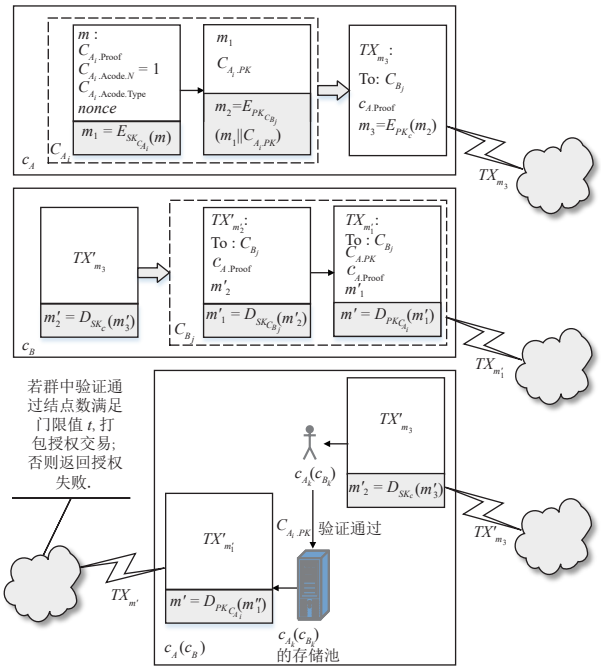


图 5 授权过程示意图

Fig. 5 Authorization diagram

(真实通信过程可能出现传输干扰、攻击等导致接收端信息异常, 因此为检测其与原始发送信号 TX_{m_3} 是否一致, 接收端用 TX'_{m_3} 表示, 后面的情况类似), 由 C_{B_j} 所在机构子群使用本文 3.1.2 节中的方法生成群私钥 $\mathcal{C}_{SK}$ 对 m'_3 解密, 得到 m'_2, C_{B_j} 使用其私钥 $C_{B_j.SK}$ 对密文 m'_2 解密, 得到密文 m'_1, 将密文 m'_1 、$C_{A_i.PK}$ 、$C_{A_i.\text{Proof}}$ 等作为交易 $TX_{m'_1}$ (即 C_{B_j} 提供的被授权证明) 在物联网联盟链系统网络广播.

建立合作关系的各联盟链内其他结点接收到 TX'_{m_3}, 将其发送给所在机构的子群验证结点, 生成群私钥 $\mathcal{C}_{SK}$ 对 m'_3 解密, 得到 m'_2. 但被授权结点外的其他结点无法对密文 m'_2 解密, 仅能提取交易中除密文外的发送者公钥及机构证明信息, 到授权链上对其所有权进行验证, 若群中超过共识门限值以上结点通过验证, 本地保存 C_{A_i} 的公钥 $C_{A_i.PK}$; 否则, 作为惩罚, 将交易发送者 C_{A_i} 加入系统黑名单, 验证结点将拒绝对黑名单中结点参与的交易进行验证 (包括 C_{A_i} 作为授权操作的被授权方或授权方).

建立合作关系的各联盟链内其他结点接收到 $TX'_{m'_1}$, 利用本地保存的 C_{A_i} 公钥 $C_{A_i.PK}$ 解密 $TX'_{m'_1}$ 中的 m'_1, 同时与利用 $TX'_{m'_1}$ 中包含的 $C_{A_i.PK}$ 解密 $TX'_{m'_1}$ 中 m'_1. 若相等, 验证 C_{B_j} 对交易 $TX'_{m'_1}$ 中授权码指定资产的操作类型和授权码中允许的操作类型是否一致, 若一致, 该结点本地验证通过. 若群中超过共识门限值以上结点通过验证, 打包授权交易, 更新授权状态链; 否则返回授权失败.

非合作联盟链内的结点接收到交易 TX'_{m_3}, 无法对密文部分解密, 忽略该交易; 若收到交易 $TX'_{m'_1}$, 因本地没有 $C_{A_i.PK}$ 仍无法对密文部分解密, 忽略该交易.

3.3 跨链原子通信

复杂跨联盟链交易机制下, 需要将一次交互过程涉及的多个交易发送给多个联盟链进行处理. 然而, 在跨链形成的链联网结构中, 如果部分联盟链共识失败或遭受 51% 攻击, 则可能出现部分联盟链接受交易而其他联盟链中止交易的情况, 链联网中错综复杂的跨链通信则会因为部分死链导致连锁式的交互失败. 如果不添加可利用的竞争条件, 将无法直接撤销已提交交易, 造成资产损失等严重后果. 为解决上述问题, 本节给出跨联盟链通信交易原子提交协议, 如图 6 所示, 包括交易初始化、锁定和解锁三个阶段, 用于原子地处理跨联盟链交易, 以防止双重支出攻击和未成功转移的价值被永久锁定, 确保各联盟链之间交易状态的一致性.

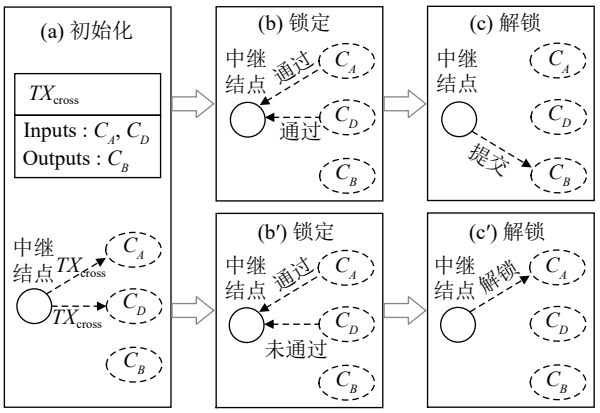


图 6 跨链原子通信示意图

Fig. 6 Cross-chain atomic communication

图 6 中, 由用户 (实体用户或智能合约用户) 账户创建并向网络广播跨联盟链交易 TX_{cross}, 假设其输入为来自两个不同联盟链的最新授权证明和交易执行逻辑, 输出为对另一联盟链的实体−资产授权关系或新生成资产的权属分配. 与交易 TX_{cross} 相关的输入联盟链运行方式如下: 在输入联盟链内部验证交易中身份证明的有效性, 若有效, 将交易锁定在该联盟链的账本中, 并广播对该交易的锁定, 允许结点访问输入联盟链账本进行交易锁定验证 (图 6 (b)); 反之, 在联盟链内创建验证未通过证明 (图 6 (b'')).

根据交易执行结果, 将对交易的解锁分为交易提交解锁和交易终止解锁. 若系统中所有联盟链都

广播了交易验收通过证明, 则可以提交相应的交易, 用户账户创建并广播解锁该交易的交易, 包括与该交易对应的锁定交易和用户账户身份证明. 然后, 各联盟链验证解锁交易, 并将原交易输出包含在输出联盟链账本的下一个块中 (图 6 (c)).

若某输入联盟链发出验证未通过证明, 则所有联盟链终止该交易. 此外, 若存在多个输入联盟链, 为了回收在其他联盟链锁定的资产, 用户账户必须向其他输入联盟链发送包含另一输入联盟链验证未通过证明的、解锁并终止该交易的请求. 其他输入联盟链收到并验证解锁请求后, 将资产标记为可再次使用 (图 6 (c')).

上述跨链原子通信协议中, 由于解锁交易要包含其他输入联盟链验证未通过证明, 因此通常比常规交易大. 在群签名共识机制下, 当超出门限值数目的联盟链验证结点在包含已提交交易的区块上达成共识时, 系统将为该交易生成群签名, 其大小与验证结点数量无关, 因此可以获得较小的解锁交易, 有助于降低存储成本并实现快速处理.

4　分析与验证

4.1　安全性分析

假设群 $\mathcal{C}$ 中实际有 t 个结点对交易 TX 进行了签名, 其中至少 t_A 个结点来自子群 $\mathcal{C}_A$, 至少 t_B 个结点来自子群 $\mathcal{C}_B$, 至少 t_D 个结点来自子群 $\mathcal{C}_D$, 则式 (21) 成立.

$$\begin{aligned} s_{\mathcal{C}} &= h(TX)\left(\sum_{p=1}^{t} f(x_i)\lambda_p + \sum_{i=1}^{t_A} g_A(y_{A_i})\mu_p + \right. \\ &\left. \sum_{j=1}^{t_B} g_B(y_{B_j})\mu_p + \sum_{k=1}^{t_D} g_D(y_{D_k})\mu_p\right) - r_{\mathcal{C}}\sum_{p=1}^{t}\mathcal{K}_p = \\ &h(TX)\left(f(0) + g_A(0) + g_B(0) + g_D(0)\right) - r_{\mathcal{C}}\sum_{p=1}^{t}\mathcal{K}_p \end{aligned} \tag{21}$$

因此有验证方程式 (22) 成立.

$$\alpha^{s_{\mathcal{C}}} {r_{\mathcal{C}}}^{r_{\mathcal{C}}} = P{K_{\mathcal{C}}}^{h(TX)} \tag{22}$$

由式 (21)、(22) 可以看出, 不在群 $\mathcal{C}$ 中的结点无法参与或干扰上述验证过程, 非合作关系的伪造跨链通信路径证明将无法得到验证, 系统忽略相应交易. 若群 $\mathcal{C}$ 中参与签名的结点数量少于 t, 有可能恢复分量 $g_X(0)$, $X \in \{A,\ B,\ D\}$, 但无法恢复分量 $f(0)$, 从而无法获得群私钥并通过验证; 若群 $\mathcal{C}$ 中参与签名的结点数量大于等于 t, 子群 $\mathcal{C}_X$ 中参与验证结点数量小于 t_X, 可以恢复分量 $f(0)$, 但无法恢复分量 $g_X(0)$, 仍无法获得群私钥并通过验证. 因此, 基于特权子群的门限群签名机制实现联盟链间交易跨链共识和结点间动态自适应授权机制, 在物联网联盟链结点身份具有确定性和可信性前提下, 能够获得较高的系统安全性.

4.2　实验部署

当前, 成熟区块链比特币每秒完成 7 笔交易, 以太坊每秒完成 15 笔交易[52]. 为对本文提出的基于可选信任–验证门限共识的动态授权机制的性能进行对比测试, 我们在 7 台服务器上构建了由 300 个虚拟验证结点组成的 Ethereum 仿真测试环境. 实验平台如下: CPU 为 Xeon-E5, 内存大小为 64 GB, 操作系统为 Ubuntu-64bit. 构造联盟链 C_A, C_B, C_D, 验证结点数 $n_A = n_B = n_D = 100$, 验证结点总数 $n = 300$, 链内共识门限值记为 t_A, t_B, t_D, 跨链共识门限值记为 t.

4.2.1　时延测试

基于存在特权子群 TDS 的共识过程主要包括结点密钥生成、密钥重构计算、共识签名以及共识签名验证 4 个部分. 预先计算结点密钥, 无需计入网络时延, 实际的网络时延主要受密钥重构计算, 共识签名以及共识签名验证计算的影响. 因此, 基于存在特权子群 TDS 的一次完整共识的实际网络时延开销计算方法为将这三者的时间开销求和处理. 此外, 我们使用 Python 设计了一个脚本, 以产生具有随机地址和足够数量的交易, 使用网络仿真模块 NetEm 手动向网络添加链路传播延迟, 用于模拟现实世界的交易发生频率.

1) 低价值交易共识时延

单链环境下, 系统以 $\Delta = 10$ ms 为时间间隔构造交易 TX, 当门限值 t_A (t_B/t_C) 以 10 为步长在区间 [10, 70] 内取不同值, 单次共识的交易数量 $\tau =$ 1, 20, 30 时, 单个低价值交易平均网络时延随门限值变化情况如图 7 (a) 所示. 可以看出, 当 $t_A \in (40,\ 70]$ 时, 网络时延显著上升; 增加单次共识的交易数量有利于提高系统吞吐量, 却也将导致单个交易平均时延增加. 将上述实验中构造交易 TX 的时间间隔设置为 $\Delta = 5$ ms, 得到单个低价值交易平均网络时延随门限值变化情况如图 7 (b) 所示. 可以看出, 降低 Δ 值对于单次共识的交易数量 $\tau = 1$ 时的共识时延影响较小, 但是显著降低了单次共识的交易数量较多时的共识时延.

2) 高价值交易共识时延

测试用例高价值交易为非跨链交易, 采用混合共识方式: 由交易所在联盟链内验证结点构成第一

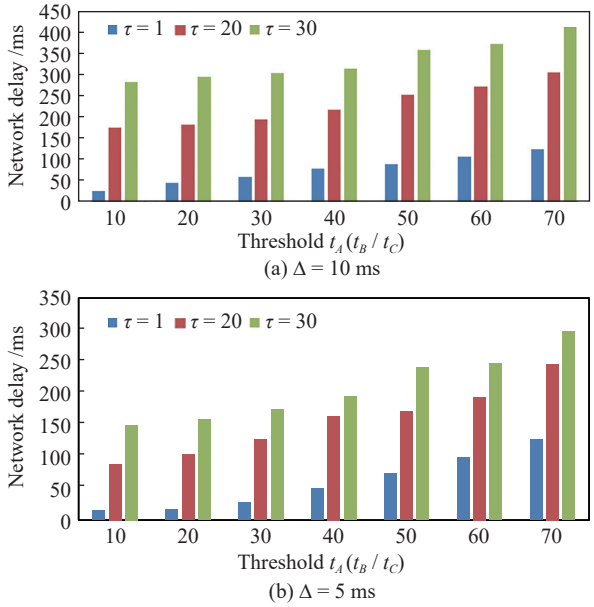


图 7 低价值交易共识时延

Fig. 7 Low-value transaction consensus delay

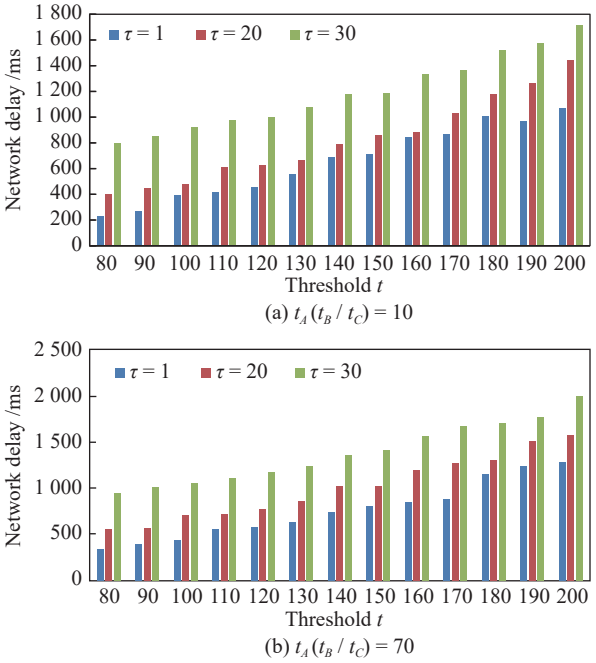


图 8 高价值交易共识时延

Fig. 8 High-value transaction consensus delay

级共识列表, 根据群签名门限值 t 随机生成来自群内各联盟链验证结点的第二级共识列表. 系统以 $\Delta = 10$ ms 为时间间隔构造交易 TX, 取第一级共识门限值 $t_A\,(t_B/t_C) = 10$, 当第二级共识门限值 t 以 10 为步长在区间 [80, 200] 内取不同值, 单次共识的交易数量 $\tau = 1$, 20, 30 时, 单个高价值交易平均网络时延随门限值 t 变化情况如图 8 (a) 所示. 可以看出, 单个高价值交易平均网络时延随着二次共识门限值的增大线性增加; 单次共识的交易数量越多, 单个交易的共识时延越大, 因此对于处理实时性要求比较高的交易可通过减少单次共识交易数量的方法降低共识时延. 将上述实验中第一级共识门限值设置为 $t_A\,(t_B/t_C) = 70$ 时, 得到单个高价值交易平均网络时延随门限值 t 变化情况如图 8 (b) 所示. 可以看出, 单个高价值交易平均网络时延有所增加, 且对单次共识的交易数量较少时影响较大.

3) 跨链交易共识时延

系统以 $\Delta = 10$ ms 为时间间隔构造仅联盟链 C_A、C_B 结点参与的跨链交易 TX, $n_A = n_B = 100$, 验证结点总数 $n = 200$, t_A, t_B 分别取 (25, 25), (50, 50), (25, 75). 由于跨链交易数目较链内交易少, 单次共识的交易数量取 $\tau = 1$, 门限值 t 以 5 为步长在区间 [100, 140] 内取不同值时, 单个跨链交易平均网络时延随门限值 t 变化情况如图 9 (a) 所示. 可以看出, 当链内共识门限值均取较小值时能够获得较低的交易时延; 参与共识验证的结点在各联盟链均匀分布时能够获得比非均匀分布时较低的交易时延.

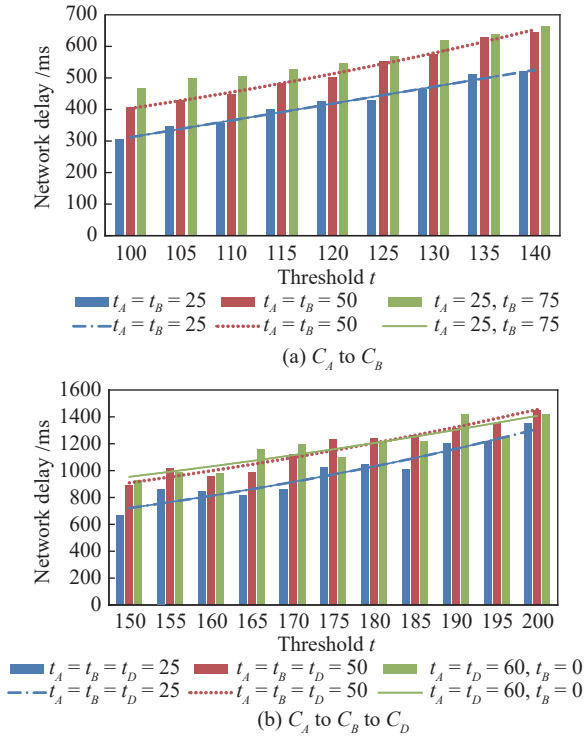


图 9 跨链交易共识时延

Fig. 9 Cross-chain transaction consensus delay

以 $\Delta = 10$ ms 为时间间隔构造联盟链 C_A, C_B, C_D 中结点参与的跨链交易 TX, 验证结点数 $n_A = n_B = n_D = 100$, 验证结点总数 $n = 300$, t_A, t_B, t_D,

分别取 (25, 25, 25), (50, 50, 50), (60, 0, 60). $t_B \neq 0$ 表示联盟链 C_B 参与测试用例中由 C_A 发送至 C_D 交易 TX 的验证; $t_B = 0$ 表示 C_B 仅作为 C_A 结点与 C_D 结点跨链通信的中继结点, 不参与交易验证. 单次共识的交易数量取 $\tau = 1$, 门限值 t 以 5 为步长在区间 [150, 200] 内取不同值时, 单个跨链交易平均网络时延随门限值 t 变化情况如图 9 (b) 所示. 可以看出, 链内共识门限值较低时, 随群共识门限值变化的单个跨链交易时延也较低; $t_B = 0$ 时单个跨链交易时延与链内共识门限值取 50 时有部分重叠且波动较大. 这是由于一方面增大链内共识门限值会引起交易时延增加; 另一方面为满足联盟链 C_A, C_B, C_D 群共识门限 t, $t_B = 0$ 时来自 C_B 实际参与群共识的验证结点数目呈现随机性, 且变化幅度较大, 从而引起来自 C_A, C_D 实际参与群共识的验证结点数目的变化较大.

4.2.2　压力测试

通过修改环境参数, 对低价值、高价值、跨链三类交易在不同构造交易时间间隔 Δ、共识门限取值下进行压力测试, 也称为系统共识吞吐量测试.

1) 低价值交易压力测试

单链环境下, $n_A\,(n_B/n_C) = 100$, 系统分别以 $\Delta = 10$ ms, $\Delta = 0$ ms (本文将系统中存在足够多待处理交易的情况看做 $\Delta = 0$ ms) 为时间间隔构造交易 TX, 链内共识门限值取 $t_A\,(t_B/t_C) = 10$, $t_A\,(t_B/t_C) = 70$, 低价值交易共识吞吐量随单次共识的交易数量 τ 变化情况如图 10 所示. 可以看出, 图中 4 种参数取值下交易吞吐量均随着单次共识的交易数量 τ 的增加而增加. $\tau = 1$, $t_A\,(t_B/t_C) = 70$, $\Delta = 0$ ms 时, 系统吞吐量仅为 8 tps, 略高于比特币; $\tau = 1$, $t_A\,(t_B/t_C) = 10$, $\Delta = 0$ ms 时, 系统吞吐量达到 37 tps, 是比特币吞吐量的约 5 倍; $\tau = 30$, $t_A\,(t_B/t_C) = 70$, $\Delta = 0$ ms 时, 系统吞吐量达到 241 tps, 是比特币吞吐量的约 34 倍, 是以太坊吞吐量的约 16 倍; $\tau = 30$, $t_A\,(t_B/t_C) = 10$, $\Delta = 0$ ms 时, 系统吞吐量达到 1 108 tps, 是比特币吞吐量的约 158 倍, 是以太坊吞吐量的约 74 倍.

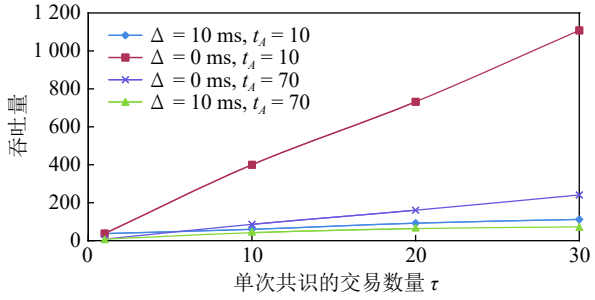


图 10　低价值交易压力测试

Fig. 10　Low-value transaction pressure test

测试结果表明, $\Delta = 0$ ms 时, 系统吞吐量受共识门限值影响较大; $\Delta = 10$ ms 时, 系统吞吐量对链内共识门限值的变化呈现一定程度的鲁棒性; 链内共识门限值较小时共识吞吐量受 Δ 影响较大.

2) 高价值交易压力测试

测试用例高价值交易为非跨链交易, 采用混合共识方式: 由交易所在联盟链内验证结点构成第一级共识列表, 根据群签名门限值 t 随机生成来自群内各联盟链验证结点的第二级共识列表. 取第一级共识门限值 $t_A\,(t_B/t_C) = 70$, 系统分别以 $\Delta = 10$ ms, $\Delta = 0$ ms 为时间间隔构造交易 TX, 第二级共识门限值分别取 $t = 100$, $t = 200$, 高价值交易共识吞吐量随单次共识的交易数量 τ 变化情况如图 11 所示. 可以看出, 图中 4 种参数取值下交易吞吐量均随着单次共识的交易数量 τ 的增加而增加. $t = 200$, $\tau = 30$, $\Delta = 0$ ms 时, 系统吞吐量达到 24 tps, 略高于比特币和以太坊的吞吐量; $t = 100$, $\tau = 30$, $\Delta = 0$ ms 时, 系统吞吐量达到 69 tps, 是比特币吞吐量的约 10 倍, 是以太坊吞吐量的约 5 倍.

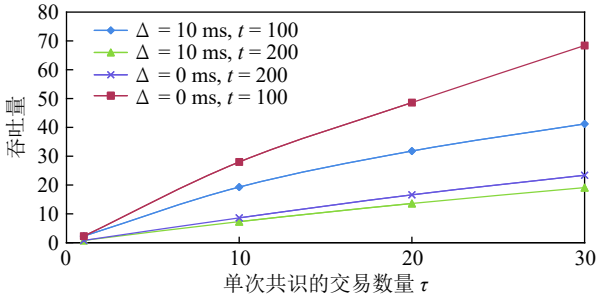


图 11　高价值交易压力测试

Fig. 11　High-value transaction pressure test

测试结果表明, 跨链共识门限值 t 较小时, 系统获得较高吞吐量; t 较大时, 系统吞吐量对 Δ 值的变化呈现一定程度的鲁棒性.

3) 跨链交易压力测试

$n_A = n_B = 100$, 验证结点总数 $n = 200$, 系统以 $\Delta = 10$ ms, $\Delta = 0$ ms 为时间间隔构造仅联盟链 C_A, C_B 结点参与的跨链交易 TX, t_A, t_B 分别取 (25, 25), (50, 50), 单次共识的交易数量取 $\tau = 1$, 群共识门限值 t 以 10 为步长在区间 [100, 140] 内取不同值时, 上述 Δ 和 t_A, t_B 的 4 种取值下系统共识吞吐量随群共识门限值 t 变化情况如图 12 (a) 所示. 可以看出, 图中 4 种情况下交易吞吐量均随群共识门限值 t 的增加而减少. $\Delta = 0$ ms, $t_A = t_B = 25$, $t = 100$

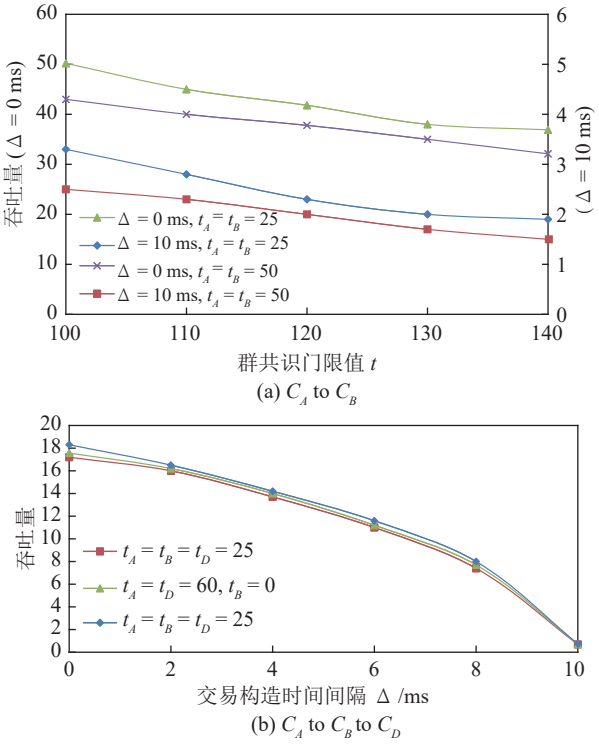


图 12 跨链交易压力测试

Fig. 12 Cross-chain transaction pressure test

时, 系统吞吐量最高达到 50 tps, 是比特币吞吐量的约 7 倍, 是以太坊吞吐量的约 3 倍.

实验结果表明, Δ 的取值对跨链交易吞吐量影响较大. 这说明当前机器计算水平下执行密码算法占交易总周转时间比重较少, Δ 取较大值时, 系统吞吐量显著减少, 且系统吞吐量对链内共识门限值的变化呈现一定的鲁棒性.

联盟链 C_A, C_B, C_D, 群共识门限值取 $t = 200$, 链内共识门限值 t_A, t_B, t_D 分别取 (25, 25, 25), (50, 50, 50), (60, 0, 60), 单次共识的交易数量取 $\tau = 1$, 构造跨联盟链 C_A, C_B, C_D 交易 TX 的时间间隔 Δ 以 2 ms 为步长在区间 [0, 10] 内取不同值时, 系统吞吐量随 Δ 变化的情况如图 12 (b) 所示. 可以看出, 设定的三种不同链内共识门限取值下, 吞吐量均随着 Δ 的增大而减小, 特别是当 $\Delta \to 10^+$, 系统吞吐量显著减少. $\Delta = 0$ ms, $t = 200$, $t_A = t_B = t_D \in [25, 50]$ 时, 系统吞吐量约为 18 tps, 略高于比特币和以太坊吞吐量. 实验表明, 群共识门限值取较大值 $t = 200$ 时, 链内共识门限值的变化对系统吞吐量呈现一定程度的鲁棒性.

综上, 在测试环境下, 本文方案处理低价值交易的系统吞吐量明显高于比特币、以太坊的吞吐量, 可以满足大部分物联网轻量级、低价值交易的效率需求. 相比处理低价值交易的系统吞吐量, 处理高价值交易和跨链交易的系统吞吐量有所降低, 但大大提升了系统安全性. 此外, 上述性能是在较强的安全约束条件下得到的, 在实际物联网应用环境中, 通过设置合理的共识门限值、单次共识交易数量等参数, 本文方案将可以获得更好的性能.

5 结论

本文通过对物联网联盟链链间交互场景进行分析, 构建了复杂情况下物联网联盟链链间通信模型, 从基于 TCCM 的链间动态授权、可选信任–验证门限共识、跨链原子通信三方面进行改进, 给出一种新型的解决复杂跨联盟链实体细粒度动态自主授权问题、由跨链操作的异步性带来的交易阻塞和失效蔓延攻击问题的通信机制. 分析及实验表明, 本文提出的跨联盟链动态通信机制能够在不牺牲安全性和吞吐量的情况下, 实现低价值交易的实时确认, 同时保障跨链交易和高价值交易的安全性.

References

1 Díaz M, Martín C, Rubio B. State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. *Journal of Network and Computer Applications*, 2016, **67**: 99–117

2 McKinsey & Company. Tech-enabled transformation: The trillion-dollar opportunity for industrials [Online], available: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/tech-enabled-transformation, December 20, 2018

3 Li H X, Zhu H J, Du S G, Liang X H, Shen X M. Privacy leakage of location sharing in mobile social networks: Attacks and defense. *IEEE Transactions on Dependable and Secure Computing*, 2018, **15**(4): 646–660

4 Zhou L, Du S G, Zhu H J, Chen C L, Ota K, Dong M X. Location privacy in usage-based automotive insurance: Attacks and countermeasures. *IEEE Transactions on Information Forensics and Security*, 2019, **14**(1): 196–211

5 Li Ji-Rui, Li Xiao-Yong, Gao Ya-Li, Gao Yun-Quan, Fang Bin-Xing. Review on data forwarding model in internet of things. *Journal of Software*, 2018, **29**(1): 196–224
(李继蕊, 李小勇, 高雅丽, 高云全, 方滨兴. 物联网环境下数据转发模型研究. 软件学报, 2018, **29**(1): 196–224)

6 Bertino E. Data security and privacy in the IoT. In: Proceedings of the 19th International Conference on Extending Database Technology. Bordeaux, France: OpenProceedings, 2016. 3–10

7 Zhang Yu-Qing, Wang Xiao-Fei, Liu Xue-Feng, Liu Ling. Survey on cloud computing security. *Journal of Software*, 2016, **27**(6): 1328–1348
(张玉清, 王晓菲, 刘雪峰, 刘玲. 云计算环境安全综述. 软件学报, 2016, **27**(6): 1328–1348)

8 Chung K, Park R C. P2P cloud network services for IoT based disaster situations information. *Peer-to-Peer Networking and Applications*, 2016, **9**(3): 566–577

9 Teing Y Y, Dehghantanha A, Choo K K R, Yang L T. Forensic investigation of P2P cloud storage services and backbone for IoT

networks: BitTorrent sync as a case study. *Computers & Electrical Engineering*, 2017, **58**: 350−363

10 Hussein D, Bertin E, Frey V. A community-driven access control approach in distributed IoT environments. *IEEE Communications Magazine*, 2017, **55**(3): 146−153

11 Yuan Yong, Zhou Tao, Zhou Ao-Ying, Duan Yong-Chao, Wang Fei-Yue. Blockchain technology: From data intelligence to knowledge automation. *Acta Automatica Sinica*, 2017, **43**(9): 1485−1490
(袁勇, 周涛, 周傲英, 段永朝, 王飞跃. 区块链技术: 从数据智能到知识自动化. 自动化学报, 2017, **43**(9): 1485−1490)

12 Zhu Jian-Ming, Ding Qing-Yang, Gao Sheng. Distributed framework of SWIFT system based on permissioned blockchain. *Journal of Software*, 2019, **30**(6): 1594−1613
(朱建明, 丁庆洋, 高胜. 基于许可链的 SWIFT 系统分布式架构. 软件学报, 2019, **30**(6): 1594−1613)

13 Landau S. Making sense from Snowden: What′s significant in the NSA surveillance revelations. *IEEE Security & Privacy*, 2013, **11**(4): 54−63

14 Yuan Yong, Wang Fei-Yue. Blockchain: The state of the art and future trends. *Acta Automatica Sinica*, 2016, **42**(4): 481−494
(袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, **42**(4): 481−494)

15 Zhu Lie-Huang, Gao Feng, Shen Meng, Li Yan-Dong, Zheng Bao-Kun, Mao Hong-Liang, et al. Survey on privacy preserving techniques for blockchain technology. *Journal of Computer Research and Development*, 2017, **54**(10): 2170−2186
(祝烈煌, 高峰, 沈蒙, 李艳东, 郑宝昆, 毛洪亮, 等. 区块链隐私保护研究综述. 计算机研究与发展, 2017, **54**(10): 2170−2186)

16 Fraga-Lamas P, Fernández-Caramés T M. A review on blockchain technologies for an advanced and cyber-resilient automotive industry. *IEEE Access*, 2019, **7**: 17578−17598

17 Fernández-Caramés T M, Fraga-Lamas P. Design of a fog computing, blockchain and IoT-based continuous glucose monitoring system for crowdsourcing mHealth. In: Proceedings of the 5th International Electronic Conference on Sensors and Applications. MDPI, 2018. 37

18 Conoscenti M, Vetro A, De Martin J C. Blockchain for the internet of things: A systematic literature review. In: Proceedings of the 13th International Conference of Computer Systems and Applications. Agadir, Morocco: IEEE, 2017. 1−6

19 Zhu Li, Yu Huan, Zhan Shi-Xiao, Qiu Wei-Wei, Li Qi-Lei. Research on high-performance consortium blockchain technology. *Journal of Software*, 2019, **30**(6): 1575−1593
(朱立, 俞欢, 詹士潇, 邱炜伟, 李启雷. 高性能联盟区块链技术研究. 软件学报, 2019, **30**(6): 1575−1593)

20 Miraz M H, Donald D C. Atomic cross-chain swaps: Development, trajectory and potential of non-monetary digital token swap facilities. *Annals of Emerging Technologies in Computing*, 2019, **3**(1): 42−50

21 Zeng Shuai, Yuan Yong, Ni Xiao-Chun, Wang Fei-Yue. Scaling blockchain towards Bitcoin: Key technologies, constraints and related issues. *Acta Automatica Sinica*, 2019, **45**(6): 1015−1030
(曾帅, 袁勇, 倪晓春, 王飞跃. 面向比特币的区块链扩容: 关键技术, 制约因素与衍生问题. 自动化学报, 2019, **45**(6): 1015−1030)

22 Redman J. Engineers demonstrate Zcash/Bitcoin atomic swaps [Online], available: https://news.bitcoin.com/engineers-demonstrate-zcashbitcoin-atomic-swaps/, October 1, 2017

23 Liu Ao-Di, Du Xue-Hui, Wang Na, Li Shao-Zhuo. Blockchain-based access control mechanism for big data. *Journal of Software*, 2019, **30**(9): 2636−2654
(刘敖迪, 杜学绘, 王娜, 李少卓. 基于区块链的大数据访问控制机制. 软件学报, 2019, **30**(9): 2636−2654)

24 Liu Ao-Di, Du Xue-Hui, Wang Na, Li Shao-Zhuo. Research progress of blockchain technology and its application in information security. *Journal of Software*, 2018, **29**(7): 2092−2115
(刘敖迪, 杜学绘, 王娜, 李少卓. 区块链技术及其在信息安全领域的研究进展. 软件学报, 2018, **29**(7): 2092−2115)

25 Qiao Rui, Cao Yan, Wang Qing-Xian. Traceability mechanism of dynamic data in internet of things based on consortium blockchain. *Journal of Software*, 2019, **30**(6): 1614−1631
(乔蕊, 曹琰, 王清贤. 基于联盟链的物联网动态数据溯源机制. 软件学报, 2019, **30**(6): 1614−1631)

26 Qiao R, Zhu S F, Wang Q X, Qin J. Optimization of dynamic data traceability mechanism in internet of things based on consortium blockchain. *International Journal of Distributed Sensor Networks*, 2018, **14**(12): 1−15

27 Qiao R, Luo X Y, Zhu S F, Liu A D, Yan X Q, Wang Q X. Dynamic autonomous cross consortium chain mechanism in e-healthcare. *IEEE Journal of Biomedical and Health Informatics*, 2020, **24**(8): 2157−2168

28 Adamik F, Kosta S. SmartExchange: Decentralised trustless cryptocurrency exchange. In: Proceedings of the 2018 International Conference on Business Information Systems. Berlin, Germany: Springer, 2018. 356−367

29 Buterin V. Chain interoperability [Online], available: https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf, September 9, 2018

30 Wang H, Cen Y Y, Li X F. Blockchain router: A cross-chain communication protocol. In: Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications. Jeju, South Korea: ACM, 2017. 94−97

31 Liu X, Zhu Q K. An intelligent value chain model with internet enterprises based on blockchain. In: Proceedings of the 2018 IEEE Advanced Information Technology, Electronic and Automation Control Conference. Chongqing, China: IEEE, 2018. 1845−1849

32 Borkowski M, McDonald D, Ritzer C, Schulte S. Towards atomic cross-chain token transfers: State of the art and open questions within TAST [Online], available: http://www.borkowski.at/pub/tast-white-paper-1.pdf, October 7, 2018

33 Li Fang, Li Zhuo-Ran, Zhao He. Research on the progress in cross-chain technology of blockchains. *Journal of Software*, 2019, **30**(6): 1649−1660
(李芳, 李卓然, 赵赫. 区块链跨链技术进展研究. 软件学报, 2019, **30**(6): 1649−1660)

34 Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments [Online], available: https://lightning.network/lightning-network-paper.pdf, December 14, 2019

35 Piatkivskyi D, Axelsson S, Nowostawski M. Digital forensic implications of collusion attacks on the lightning network. In: Proceedings of the 13th IFIP International Conference on Digital Forensics. Orlando, USA: Springer, 2017. 133−147

36 BlockStream [Online], available: https://blockstream.com/, December 5, 2019

37 Back A, Corallo M, Dashjr L, Friedenbach M, Maxwell G, Miller A, et al. Enabling blockchain innovations with pegged sidechains [Online], available: https://www.blockstream.com/sidechains.pdf, November 23, 2019

38 RootStock [Online], available: https://www.rsk.co/, October 11, 2019

39 Lisk [Online], available: https://lisk.io/, October 15, 2019

40 Asch [Online], available: https://www.asch.io/, November 2, 2018

41 Vitalik B. Ethereum sharding faq [Online], available: https://github.com/ethereum/wiki/wiki/Sharding-FAQs, November 17, 2018

42 Thomas S, Schwartz E. A protocol for interledger payments [Online], available: https://interledger.org/interledger.pdf, December 18, 2019

43 Pointnity Network [Online], available: http://pointnity.network/, December 22, 2018

44 Wood G. Polkadot: Vision for a heterogeneous multi-chain framework [Online], available: https://polkadot.network/PolkaDotPaper.pdf, October 22, 2018

45 Fusion [Online], available: https://fusion.org/, November 29, 2018

46 Buterin V. A next generation smart contract & Decentralized application platform [Online], available: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf, December 11, 2017

47 He Hai-Wu, Yan An, Chen Ze-Hua. Survey of smart contract technology and application based on blockchain. *Journal of Computer Research and Development*, 2018, **55**(11): 2452−2466 (贺海武, 延安, 陈泽华. 基于区块链的智能合约技术与应用综述. 计算机研究与发展, 2018, **55**(11): 2452−2466)

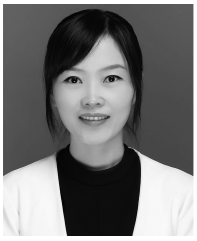
48 Etherscan. Ethereum unique address growth chart [Online], available: https://etherscan.io/chart/address/, December 28, 2019

49 Park D, Zhang Y, Saxena M, Daian P, Rosu G. A formal verification tool for ethereum VM bytecode. In: Proceedings of the 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering. Lake Buena Vista, USA: ACM, 2018. 912−915

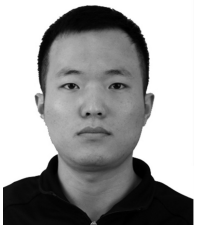
50 Warren W, Bandeali A. 0x: An open protocol for decentralized exchange on the Ethereum blockchain [Online], available: https://deepai.org/publication/enabling-cross-chain-transactions-a-decentralized-cryptocurrency-exchange-protocol, December 18, 2017

51 Aeternity [Online], available: https://aeternity.com/, November 22, 2018

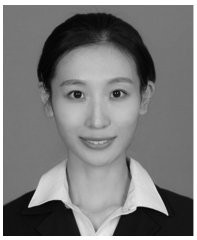
52 Cui L Z, Yang S, Chen Z T, Pan Y, Xu M W, Xu K. An efficient and compacted DAG-based blockchain protocol for industrial internet of things. *IEEE Transactions on Industrial Informatics*, 2020, **16**(6): 4134−4145



乔 蕊 周口师范学院副教授, 战略支援部队信息工程大学博士研究生. 主要研究方向为物联网安全, 区块链. 本文通信作者.
E-mail: jorui_314@126.com
(**QIAO Rui** Associate professor at Zhoukou Normal University, and Ph.D. candidate at Strategic Support Force Information Engineering University. Her research interest covers security of IoT and blockchain. Corresponding author of this paper.)



刘敖迪 战略支援部队信息工程大学博士研究生. 主要研究方向为大数据, 区块链.
E-mail: ladyexue@163.com
(**LIU Ao-Di** Ph.D. candidate at Strategic Support Force Information Engineering University. His research interest covers big data and blockchain.)



陈 迪 战略支援部队信息工程大学博士研究生. 主要研究方向为域间路由安全, 区块链.
E-mail: chendi-409@tom.com
(**CHEN Di** Ph.D. candidate at Strategic Support Force Information Engineering University. Her research interest covers interdomain security and blockchain.)

王清贤 郑州大学教授. 主要研究方向为网络与信息安全.
E-mail: wqx2008@vip.sina.com
(**WANG Qing-Xian** Professor at Zhengzhou University. His main research interest is network and information security.)