软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2021,32(4):953−972 [doi: 10.13328/j.cnki.jos.006229]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

区块链赋能的高效物联网数据激励共享方案*

蔡 婷[1,2], 林 晖[1,2], 陈武辉[1,2], 郑子彬[1,2], 余 阳[1,2]

[1](中山大学 数据科学与计算机学院,广东 广州 510006)

[2](国家数字家庭工程技术研究中心(中山大学),广东 广州 510006)

通讯作者: 陈武辉, E-mail: chenwuh@mail.sysu.edu.cn

摘 要: 近年来,随着大量设备不断地加入物联网中,数据共享作为物联网市场的主要驱动因素成为了研究热点.然而,当前的物联网数据共享存在着出于安全顾虑和缺乏激励机制等原因导致用户不愿意参与共享数据的问题.在此背景下,区块链技术为解决用户的信任问题和提供安全的数据存储被引入到物联网数据共享中.然而,在构建基于区块链的安全分布式数据共享系统的探索过程中,如何突破区块链固有的性能瓶颈仍然是一个关键挑战.为此,研究了基于区块链的高效物联网数据激励共享方案.该方案首先提出了一个高效的区块链物联网数据激励共享框架,称为 ShareBC.ShareBC 利用分片技术构建能够并行处理数据共享交易的异步共识区,并在云/边缘服务器上和分片异步共识区上部署高效的共识机制,从而提高数据共享交易的处理效率.然后,为激励物联网用户参与数据共享,提出了一种基于智能合约实现的层次数据拍卖模型的共享激励机制.该机制解决了物联网数据共享中涉及的多层数据分配有效性问题,能够最大限度地提高整体社会福利.最后,实验结果表明了该方案的经济效益、激励兼容性和实时性以及可扩展性,且具有较低的计算成本和良好的实用性.

关键词: 区块链;数据共享;分片;激励机制;物联网

中图法分类号: TP393

中文引用格式: 蔡婷,林晖,陈武辉,郑子彬,余阳.区块链赋能的高效物联网数据激励共享方案.软件学报,2021,32(4):953−972. http://www.jos.org.cn/1000-9825/6229.htm

英文引用格式: Cai T, Lin H, Chen WH, Zheng ZB, Yu Y. Efficient blockchain-empowered data sharing incentive scheme for Internet of Things. Ruan Jian Xue Bao/Journal of Software, 2021,32(4):953−972 (in Chinese). http://www.jos.org.cn/1000-9825/6229.htm

Efficient Blockchain-empowered Data Sharing Incentive Scheme for Internet of Things

CAI Ting[1,2], LIN Hui[1,2], CHEN Wu-Hui[1,2], ZHENG Zi-Bin[1,2], YU Yang[1,2]

[1](School of Data and Computer Science, Sun Yat-Sen University, Guangzhou 510006, China)

[2](National Engineering Research Center of Digital Life (Sun Yat-Sen University), Guangzhou 510006, China)

Abstract: In recent years, with a large number of devices that continuously join the IoT, data sharing as the main driver of the IoT market has become a research hotspot. However, the users are reluctant to participate in data sharing due to the security concerns and lacking of incentive mechanism in current IoT. In this context, blockchain is introduced into the data sharing of IoT to solve the trust

* 基金项目: 广东省重点领域研发计划(2019B020214006); 国家自然科学基金(62032025, 61802450); NSFC-广东联合基金集成项目(U20A6003); 广东引进创新创业团队计划(2017ZT07X355); 珠江人才招聘计划(2019QN01X130); 重庆市教委科学技术研究项目(KJZD-K201802401)

Foundation item: Key-area Research and Development Program of Guangdong Province (2019B020214006); National Natural Science Foundation of China (62032025, 61802450); NSFC-Guangdong Joint Fund Project (U20A6003); Program for Guangdong Introducing Innovative and Entrepreneurial Teams (2017ZT07X355); Pearl River Talent Recruitment Program (2019QN01X130); Science and Technology Research Program of Chongqing Municipal Education Commission (KJZD-K201802401)

本文由“面向领域的软件系统构造与质量保障”专题特约编辑潘敏学教授、魏峻研究员、崔展齐教授推荐.

收稿时间: 2020-09-13; 修改时间: 2020-10-26; 采用时间: 2020-12-19; jos 在线出版时间: 2021-01-22

© 中国科学院软件研究所 http://www.jos.org.cn

problem of users and provide secure data storage. However, in the exploration of building a secure distributed data sharing system based on the blockchain, how to break the inherent performance bottleneck of blockchain is still a major challenge. For this reason, the efficient blockchain-based data sharing incentive scheme is studied for IoT, in which an efficient data incentive sharing framework based on blockchain is proposed, named ShareBC. Firstly, ShareBC uses sharding technology to build asynchronous consensus zones that can process data sharing transactions in parallel and deploy efficient consensus mechanisms on the cloud/edge servers and asynchronous consensus zones in sharding, thus improving the processing efficiency of data sharing transactions. Then, in order to encourage IoT users to participate in data sharing, a sharing incentive mechanism based on hierarchical data auction model implemented by smart contract is presented. The proposed mechanism can effectively solve the problem of multi-layer data allocation involved in IoT data sharing, and maximize the overall social welfare. Finally, the experimental results show that the proposed scheme is economically efficient, incentive-compatible, real-time, and scalability, and has low cost and good practicability.

Key words: blockchain; data sharing; sharding; incentive mechanism; IoT

随着5G和移动云计算技术的发展,数据共享在物联网开发与应用领域日益发挥着越来越重要的作用,这是因为绝大多数的物联网应用程序底层都是基于数据共享来部署的[1].据大数据统计,物联网设备的数量在 2025 年预计上升至 416 亿台.这将意味着每秒在全球范围内将有 127 台新设备连接到互联网.这些物联网设备每天产生约 5 亿字节的数据,预计到 2025 年达到 79.4 兆字节的数据量[2,3].大胆地设想一下,这些海量数据将在物联网设备之间进行共享和分析,进而不可避免地创造一个超大规模的数据交易市场[4].然而,当前的物联网数据市场远未达到这一预期.究其原因[5−9],一方面是因为数据共享在实践过程中通常需要消耗共享参与者一定数量的资源和成本.在缺乏有效的参与者激励策略的情况下,很难平衡多方利益,因此物联网用户多数不愿意主动地共享数据或转发消息;另一方面,在大量的感知数据(如位置信息)中可能存在个体隐私泄漏的风险,诸如此类的安全问题阻碍了物联网用户加入到数据共享市场中来.

通过有效的激励机制来鼓励用户积极参与物联网数据共享是一个有效的举措.目前,已经出现了将激励机制引入移动群体感知或资源交易等物联网应用场景,并以此激励用户参与数据共享行为的相关研究[10−13].例如,Gao 等人[10]提出了一种适用于非确定性车载自组网的有效激励机制.Pu 等人[11]研究了应用于大规模车辆移动群体感知的基于激励的混合边缘计算框架.Petrov 等人[12]面向窄带物联网应用设计了基于机会主义的人群感知激励机制.然而,这些研究方法大多都是集中式的,它们在无法保证数据完整性和不可信的物联网应用中面临着安全性挑战[14].比如,在物联网中,数据服务器可能会遭受恶意用户或服务提供商的攻击,服务器中存储的数据会被篡改;不诚实的物联网用户考虑自身利益或者因非法目的而提供虚假甚至恶意数据[15].

考虑到安全挑战极其重要的特性,区块链因其固有的安全属性,如分散化、匿名化、可追踪和不可篡改性等,使其成为一项非常具有吸引力的技术被引入到物联网数据共享中,以解决物联网用户的信任问题,并提供安全的数据存储[16].许多基于区块链的物联网数据共享的相关研究工作已被提出并得以实现.例如,Kang 等人[17]通过优化共识管理机制,提出了一种基于区块链的车联网数据共享方案.Yu 等人[18]提出了一种基于 Bitcoin 的加密货币 LRCoin,其核心思想是为物联网中的数据交易设计具有抗泄漏的数字签名方案,提高数据交易的安全性.Yang 等人[19]利用贝叶斯推理模型设计了一种基于区块链的信任管理系统.这些研究都试图利用区块链技术来解决物联网应用中的数据共享问题,然而在构建基于区块链的安全分布式共享系统的探索过程中,忽略了区块链固有的关键性能瓶颈问题[20].例如,Bitcoin 最大交易吞吐量约为 7 笔/秒,创建交易的客户端平均必须等待至少 10 分钟才能够确保交易上链;Ethereum 最大吞吐量限制在 20 笔/秒,平均延迟时间为 12s.相比之下,类似于 Visa 这种中心化支付系统,通常能够在几秒钟内确认交易,其吞吐量甚至可以高达每秒上万笔[21,22].区块链的性能瓶颈已然成为又一阻碍物联网用户参与数据共享的重要因素.因此,要想利用区块链技术助力潜在的由数十亿物联网设备所组成的大规模数据共享市场,必须考虑尽可能地提高它的性能,同时保留其安全性和去中心化属性,并且迫切需要研究和提出基于区块链的高效物联网数据激励共享方案.

针对上述问题,本文首先提出了一个高效的区块链物联网数据激励共享框架,称为 ShareBC.在该体系结构中,ShareBC 引入分片技术[23]将网络中的所有物联网设备划分成若干个异步共识区,将原来需要全网节点共同进行的交易验证工作在各个分片异步共识区并行处理,以增强基于区块链的数据共享系统的交易处理能力.此

© 中国科学院软件研究所 http://www.jos.org.cn

外,根据联盟区块链和物联网数据共享的特点[24],本文为 ShareBC 设计了高效的共识过程,联盟链委员会(committee)依赖一组分布式的异步共识区并同时保持了对于数据共享交易的完全控制,这种共识机制具有强大的透明度和可审计性保证,在计算成本和可扩展性方面也具有一定的优势;另一方面,为了鼓励物联网用户参与数据共享,本文还提出了一种基于智能合约实现的层次数据拍卖模型的共享激励机制,以最大限度地提高各方参与者的整体社会福利.实践中,物联网设备间的数据共享通常面临着多层通信网络结构所带来的局限性[25],该机制因此设计了包括数据代理在内的 3 层数据拍卖模型和相应的数据分配以及定价规则,并考虑了数据传输成本对于社会福利的影响.最后,该机制通过智能合约的形式强制生效,确保了在数据共享交易中拍卖规则的不可否认性和执行效率.

本文的主要贡献总结如下:

(1) 提出了一种高效的区块链物联网数据激励共享框架——ShareBC.为了提高系统的交易处理能力,ShareBC 引入分片并给出了基于区块链的物联网数据共享的分片构建步骤.并且,ShareBC 还在分片异步共识区和云/边缘服务器上部署了高效的共识机制,避免了传统的基于工作量证明方式生成区块所导致的高计算开销问题,提升了共识生成区块的效率;

(2) 提出了一种基于智能合约的层次数据拍卖模型的物联网数据共享激励机制.为确保尽可能多的物联网设备参与数据共享,该机制基于 ShareBC 框架提出 3 层数据拍卖模型,其中,通信受限的底层设备可以通过数据代理的帮助间接地访问数据共享资源,从而实现社会福利的最大化;

(3) 开发了原型系统.为了简化拍卖机制的逻辑,拍卖智能合约被分层设计且分别部署在 3 层数据拍卖模型中,测试结果表明,智能合约的计算成本较低,具有良好的实用性.最后,大量的仿真实验表明了共享激励机制的经济效益、激励兼容性和实时性以及可扩展性.

1 相关工作

1.1 集中式物联网数据激励共享

随着物联网采集数据的爆发式增长,物联网数据共享研究受到学术界的广泛关注[26−33].例如,Wang 等人[26]提出了适用于车辆轨迹预测的车载自组网数据共享参与者招募策略,最大程度地降低了总招募成本.Ni 等人[27]提出一种基于雾计算的移动群体感知框架以解决任务请求者与工人之间的安全和隐私问题.Xiao 等人[28]研究了基于博弈论的车联网数据共享问题,利用 Q-Learning 算法实现车辆报酬支付策略.然而,在这些研究工作中还缺乏有效的激励机制,大多数方案中物联网实体的数据共享行为是出于自愿和主动性假设,显然,这是违背客观事实的.为了解决物联网设备之间数据共享的激励问题,各种单层拍卖机制先后被提出.例如,在文献[31]中,Jin 等人提出一种激励兼容的拍卖机制,根据移动设备的需求确定资源报价,实现移动设备(买家)与云服务提供商(卖家)之间的资源共享交易.在文献[32]中,Wen 等人提出一种质量驱动的拍卖激励机制,该机制能够根据感知数据的质量计算参与者的支付费用,以提高用户参与收集和共享感知数据的积极性.

单层拍卖机制在大规模的物联网数据激励共享场景中存在着应用上的局限性[30].这是因为,在无线网络中智能物联网设备的地理位置分散且数据共享服务覆盖范围有限,部分终端设备因通信和服务受限而无法加入数据市场,需要其他物联网设备充当中间代理以帮助其获取共享数据资源,单层拍卖模型显然已经无法针对这种层次结构场景进行建模并求解最大化社会福利.在此问题背景下,层次拍卖机制作为一种能够实现物联网共享设备之间社会福利最大化的极具前景的解决方案被提了出来.例如,Kiani 等人[29]研究并提出基于动态规划问题的 3 层资源分配模型.Wang 等人[30]提出一种适用于多机器人实时通信和高效数据检索的多层拍卖机制.然而,大部分传统激励机制下的数据共享模型都是集中式的,它们通常依赖于可信的第三方中心化机构,存在很大的被攻击风险且易导致单点故障.此外,不诚实用户可能因为自身利益等原因提供虚假甚至恶意数据,进一步加剧了数据共享的信任危机[34].

© 中国科学院软件研究所 http://www.jos.org.cn

1.2 基于区块链的物联网数据共享及激励机制应用

基于区块链的分布式系统被认为是建立安全和可信数据共享的有效技术[2,35−38].例如,Li 等人[36]实现了一种基于区块链的移动群体感知系统,该系统支持任务请求者直接将任务发送给工人,避免了传统集中式的可信第三方平台的涉入.Cai 等人[16]利用门限签名技术开发了基于区块链的社交链接数据的可信访问认证系统,该系统的关注点在于数据共享和隐私保护,这同样适用于物联网中的数据共享应用.然而,绝大多数的现有工作只是简单地将区块链应用于物联网中以构建安全的数据共享系统,忽略了区块链自身的性能瓶颈,这一问题在本文研究中将给予重点考虑;另一方面,在激励机制方面,区块链技术已经与各种单层资源分配协议相结合.例如,He 等人[37]提出一种真实的激励机制,能够满足动态和分布式 P2P 环境中物联网用户的不同资源分配需求.Kang 等人[38]提出一种本地 P2P 电力资源共享模型,支持在混合动力车辆之间进行本地电力买卖交易.Yao 等人[2]利用区块链构建了去中心化的工业物联网设备自组织交易平台,并将设备之间的共享交易行为建模为斯塔克伯格博弈.然而,在这些现有研究中鲜有基于区块链驱动的多层拍卖激励机制的探索.研究具有层次结构的拍卖模型,解决基于区块链架构中的物联网多层数据共享安全、效率以及激励问题,这将是本文工作与现有研究的主要区别.

2 高效的区块链物联网数据激励共享框架(ShareBC)

ShareBC 本质上是激励机制和区块链技术的融合.为了提升区块链系统的共识效率,ShareBC 提出在联盟链的基础上通过分片技术使部分节点并行地工作以替代传统的全网共识方式,避免了在公共无许可区块链中基于 PoW(proof-of-work)共识机制所导致的高计算开销问题[22,23].在本节中,首先描述 ShareBC 的组成实体.然后,提出基于 ShareBC 实现的数据共享过程和关键步骤.

2.1 框架描述

如图 1 所示,ShareBC 包括 3 类物联网共享实体:数据提供者、数据代理和数据用户.

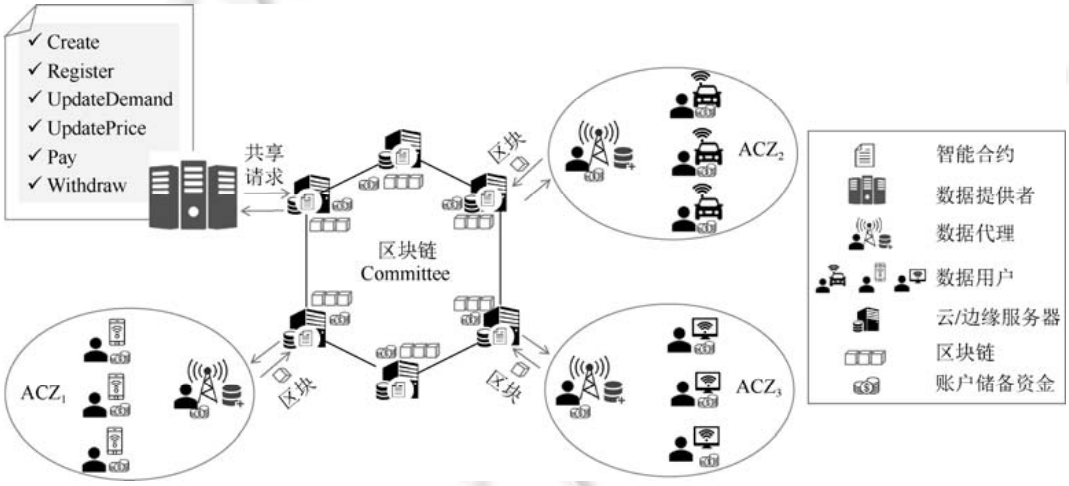


Fig.1 Efficient blockchain-based data sharing incentive framework for IoT (ShareBC)

图 1 高效的区块链物联网数据激励共享框架(ShareBC)

其中,数据提供者是拥有共享数据资源的物联网设备;数据代理和数据用户均为具有数据需求的物联网设备.在假设场景中,每个物联网数据用户直接连接到附近的数据代理并通过其与云/边缘服务器进行通信.每个物联网数据用户只能连接到唯一的数据代理,因此与该数据代理所连接的所有数据用户将被划分为同一个区域,称为异步共识区(asynchronous consensus zone,简称 ACZ).此外,每个数据代理和数据用户都配置有独立的共

© 中国科学院软件研究所 http://www.jos.org.cn

享交易账户,账户地址被要求设置为无关用户个体隐私的信息,如:公开密钥.在 ShareBC 激励共享机制中,数据提供者通过云/边缘服务器发布数据共享请求交易.随后,在由云/边缘服务器组成的拍卖平台接收到数据提供者的注册信息后,采用层次数据拍卖机制根据购买需求、拍卖价格以及传输数据成本决定数据代理和数据用户分别能够获得的共享数据数量和支付价格.然后,数据代理和数据用户访问各自拍卖所得的数据资源并完成相应的支付.最后,这些数据共享交易记录在分片 ACZ 中被打包成区块,由预选的联盟链委员会完成最终审计并在达成共识后添加到区块链上.

2.2 基于ShareBC实现的数据共享关键步骤

2.2.1 系统初始化

系统初始化阶段包括物联网设备注册和智能合约部署两个步骤.首先,在系统建立后,可信中心(cerfificate authority,简称 CA)会初始化系统参数并利用非对称密码技术为新注册的物联网设备生成对应的公钥和私钥.出于安全考虑,私钥在发送给用户后会及时销毁,公钥则作为物联网设备在系统中的唯一标识存在.考虑到联盟链中对于匿名交易的可监管需求,CA 通过存储物联网设备真实身份信息和公钥的映射关系关联表从而实现可监管的匿名认证方案[39].这样,当物联网数据用户身份认证出现争端时,其数据代理可以请求 CA 进行仲裁并追踪其真实身份.其次,完成智能合约的编译和部署.ShareBC 使用智能合约自动执行数据共享交易过程.在区块链网络中初始化智能合约后,数据提供者可以参与订制数据共享激励机制.一旦部署成功,智能合约将拥有独立 ID 并被永久性地记录在区块链中.

2.2.2 分片构建

ShareBC 引入分片[23]的目的是将网络中的所有物联网设备分成若干个子网络,将原来需要全网节点共同进行的交易验证工作在各个分片网络区域内并行处理,从而增强区块链系统交易处理能力.具体来说,构建分片包括如下主要步骤.

(1) 网络分片:根据物联网设备的某个关键特征值(如地理坐标范围)将其划分成不同的分片 ACZ.每个分片 ACZ 是同质的,其功能一样且地位平等.考虑到容错性,每个分片 ACZ 中的节点数量存在阈值;

(2) 节点分工:分片 ACZ 通过内部的物联网设备共同进行数据交易的验证工作.在分片 ACZ 中,物联网设备节点会进行相应的分工,从中选取 1 个领导(leader)节点和若干个普通(follower)节点.为确保分片安全性,每执行一轮动作周期后需要重新选举下一轮 leader 节点.考虑到联盟链的特性,首轮每个分片 ACZ 中的 leader 节点可以预指定.以后每轮 leader 节点的选取可以通过基于随机数的计算方式[22]进行随机确定;

(3) 增加或减少分片:针对新物联网设备加入和原有节点的移动问题,ShareBC 规定每个分片 ACZ 中的节点数量阈值是固定的.每个分片 ACZ 中拥有的节点数量与该分片 ACZ 的权重成正比,确保在分片数量增加或减少后分片 ACZ 之间仍然能够保持均衡性.例如,当前分片 ACZ 工作负载较高时,可以通过增加分片的方式提高系统吞吐量.若当前分片 ACZ 中节点数量低于安全阈值,则可取消该分片 ACZ 并迁移区域内节点至其他分片 ACZ.

2.2.3 物联网设备的角色设定

在图 1 模拟的数据激励共享场景中,数据提供者可以利用区块链网络广播其数据交易请求,并通过共享数据获得报酬.数据需求者则包括两类角色:数据代理和数据用户.考虑到分片 ACZ 内节点通信受地理位置影响并且数据共享服务覆盖区域有限,在 ShareBC 中规定:数据用户不能直接向数据提供者请求交易并获得共享数据,它需要通过其所在分片 ACZ 的数据代理作为中间方帮助其获得;数据代理可以直接与数据提供者进行数据交易从而获取共享数据资源.

2.2.4 基于智能合约的数据激励共享机制

图 1 中展示了智能合约 6 个主要的功能接口,物联网数据共享的关键事件将通过调用这些接口自动执行.数据提供者首先调用智能合约的 Register 接口注册共享数据资源服务,然后,数据代理调用 Register 接口加入数据共享交易.在 Register 接口中,智能合约定义了数据共享机制的所有相应变量,如数据资源集的数量 D、初始数据报价 p、数据价格增量 C 和数据需求 $\boldsymbol{r}$.在两者完成注册后,智能合约即创建了在数据提供者与数据代理之

© 中国科学院软件研究所 http://www.jos.org.cn

间交易数据的顶层市场.接下来,数据代理将通过智能合约 Create 接口创建子合约 $\mathcal{H}'$, 并建立与其分片 ACZ 中数据用户之间数据交易的底层市场,其中,数据用户则通过子合约 $\mathcal{H}'$ 的 Register 接口加入到数据共享交易中.

在完成上述步骤后,数据提供者、数据代理和数据用户可以开始数据共享.为了最大限度地提高社会福利,激励物联网设备积极地参与数据共享交易,智能合约提供了 UpdateDemand 接口.分片 ACZ 中数据用户可以通过合约 $\mathcal{H}'$ 的 UpdateDemand 接口更新其数据需求,当收集足够的底层数据需求时,数据代理调用智能合约 $\mathcal{H}$ 的 UpdateDemand 接口更新它在顶层市场的数据需求.当数据交易供需相等时,拍卖结束.在此之前,智能合约提供了 UpdatePrice 接口供数据提供者更新数据报价并进入新一轮拍卖.对于每个赢家设备(数据代理和数据用户),需要通过 Pay 接口向数据提供者进行支付.拍卖结束后,数据代理和数据用户可以通过 Withdraw 接口取回剩余的账户资金.

2.2.5 激励共享数据访问和交易生成

赢家数据代理(数据用户)从数据提供者(数据代理)下载对应的共享数据资源,完成解密并实现共享数据的访问.为了确保数据资源在转卖过程中的安全性,数据提供方可采用一次性密码(one-time password,简称 OTP)[40]技术对共享数据进行加密.这样,就能够有效地避免数据代理从数据提供方拍卖获取到数据资源后又转卖给数据用户所形成的多次收益.在被智能合约广播提交之后,意味着该笔数据共享交易完成.每笔数据共享交易由交易信息和数字签名两部分构成[35],其中,交易信息包括支付记录、交易开销和交易生成的时间戳.考虑到区块链系统存储的有限性,交易数据中往往包含一个索引,用于记录加密过的共享数据的链外存储位置;数字签名则是由交易双方的私钥签署生成.最后,在分片 ACZ 节点收集一定数量的交易记录后,这些交易将被打包成一个区块并进入下面的共识过程.

2.2.6 共识过程

基于 ShareBC 的区块链共识过程主要包括两个阶段:首先,在分片 ACZ 内部完成交易验证并共识出区块.每一个分片都可以选择该区域内的共识算法[20](例如,PoW、PoS、PoB 或者 PBFT);然后,在分片之间会根据某种预定的协议达成共识,实现分片互联的全局系统.如图 2 所示为本文所提出的物联网数据共享框架的区块链共识过程,其两个阶段都采用了实用拜占庭容错(practical Byzantine fault tolerance,简称 PBFT)类型的共识算法.以图 2(a)为例,每个分片 ACZ 内部节点的共识过程分为生成块、预准备、准备、确认和响应这 5 个步骤.

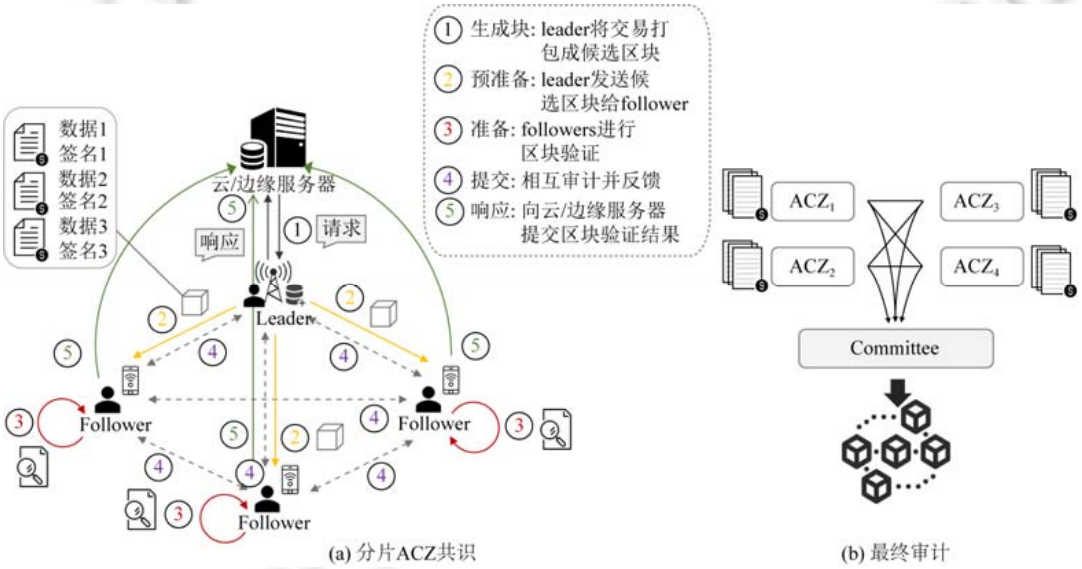


Fig.2 ShareBC based blockchain consensus processe

图 2 基于 ShareBC 框架的区块链共识过程

- 生成块:完成的数据共享交易将由网络中全部节点所验证,被确认无误的交易将由这些验证节点进行签名并提交其对应分片 ACZ 中的 leader 节点.在每个分片 ACZ 中,由 leader 节点负责将收集到的确认交易打包成候选区块;
- 预准备:每个 leader 节点管理一个唯一列表,其记录了当前轮周期中该分片 ACZ 内部所有 follower 节点的信息.根据这个列表,leader 节点在当前阶段会将候选区块转发给它所在分片 ACZ 中的 follower 节点以进行共识;
- 准备:每个接收到消息的 follower 节点将验证候选区块的有效性;
- 确认:每个 follower 节点完成候选块的验证,并将附有自己签名的反馈消息广播给分片 ACZ 内的其他节点.若超过一定数量(如 2/3 节点总数)的 follower 节点达成共识,则进入提交阶段并广播提交请求.否则,leader 节点会根据反馈结果考虑是否发起下一轮共识;
- 响应:分片 ACZ 中 leader 节点将达成共识的候选区块提交给委员会完成最终审计.

在完成上述步骤后,共识出区块的分片 ACZ 中 leader 节点会通过附近的云/边缘服务器将候选区块提交给联盟链委员会进行最终审计,如图 2(b)所示.在 ShareBC 中,委员会由联盟链主体提供的一组云/边缘服务器组成.委员会节点之间通过运行 PBFT 共识协议完成对候选区块的最终审计,审计通过的候选区块将被作为新区块添加到区块链上并随后被同步广播给网络中的其他分片 ACZ.此外,Committee 同时负责在每一轮中生成一个计算随机数用于选取分片 ACZ leader 节点.在这种共识机制中,Committee 依赖分布式分片 ACZ 并同时保持了对于数据共享交易的完全控制,具有强大的透明度和可审计性保证,在计算成本和可扩展性方面也具有优势,分片内部共识细节将在第 4.1 节中进行详细阐述.

3 数据共享激励机制

如何设计有效的激励机制驱动物联网用户积极地参与数据共享是本文的另一个研究重点.在 ShareBC 的基础上,本文提出了一种基于智能合约实现的层次数据拍卖模型的共享激励机制,该机制能够最大化参与者的社会福利并保证共享交易效率.在本节中,首先对物联网中的数据共享问题进行抽象;然后,给出其形式化表示;之后,对其研究问题进行定义,提出层次数据拍卖的数学模型.在此基础上,提出基于智能合约实现的 3 层数据拍卖算法;最后,给出相关算法定理证明.

3.1 问题描述

基于区块链的物联网数据共享问题可以抽象为 1 个层次数据交易市场,如图 3 所示.该交易市场主要由数据提供者 $\mathcal{P}$、数据代理 $\mathcal{M}=\{1,2,...,M\}$ 和数据用户 $\mathcal{N}=\{1,2,...,N\}$ 组成.其中,$\mathcal{P}$ 和 $\mathcal{M}$ 构成数据共享交易的顶层市场,$\mathcal{M}$ 和 $\mathcal{N}$ 形成底层市场.假设共享的数据资源是可分割且同质的,设 $\mathcal{D}=\{1,2,...,D\}$ 为 $\mathcal{P}$ 所拥有的共享数据资源,其中,D 表示一个整数.每个数据代理 $j\in\mathcal{M}$ 对数据集 $\mathcal{D}$ 的效用向量定义为 $\mathbf{u}_j$,这与该数据代理在其所属的分片 ACZ 中转卖数据所获得的收益相同,其中,$\mathcal{N}_j$ 表示数据代理 j 所在分片 ACZ 中的数据用户集合.注意,$j\in\mathcal{N}_j$,这是因为数据代理 j 也可以在底层市场中作为数据用户参与数据交易.每个数据用户 $i\in\mathcal{N}_j$ 对数据集 $\mathcal{D}$ 的效用向量定义为 $\mathbf{v}_i$,根据边际效用递减原理,$\mathbf{v}_i$ 中的元素排列顺序是按值递减的.考虑数据资源的可分割性,假设数据用户 i 访问的第 k 个数据资源的大小为 $D_i[k]$.

系统规定在一笔数据共享交易生效之后,访问数据需要通过数据代理连接到数据提供者进行数据资源的下载.物联网数据用户必须通过其所在分片 ACZ 中的数据代理帮助其获得数据提供者的共享数据.假设通信双方的网络通道容量表示为 $H_{i,j}$,数据用户(或数据代理) $i\in\mathcal{N}\cup\mathcal{M}$ 从数据代理(或数据提供者) $j\in\mathcal{M}\cup\mathcal{P}$ 访问第 k 个数据资源所需要的传输时间为

$$T_{i,j}(D_i[k])=D_i[k]/H_{i,j} \tag{1}$$

根据 Hong 等人[9]的计算方法,传输能耗定义为数据用户或者数据代理的传输功率与传输时间的乘积.假设通信双方之间的传输功率表示为 $P_{i,j}$,数据用户(或数据代理) $i\in\mathcal{N}\cup\mathcal{M}$ 从数据代理(或数据提供者) $j\in\mathcal{M}\cup\mathcal{P}$

© 中国科学院软件研究所 http://www.jos.org.cn

访问第 k 个数据资源所消耗的传输能量为

$$E_{i,j}(D_i[k]) = P_{i,j}T_{i,j}(D_i[k]) \tag{2}$$

根据公式(1)和公式(2),数据用户(或数据代理) $i \in \mathcal{N} \cup \mathcal{M}$ 从数据代理(或数据提供者) $j \in \mathcal{M} \cup \mathcal{P}$ 访问第 k 个数据资源所需要的传输成本表示为

$$C_{i,j}(D_i[k]) = f^E E_{i,j}(D_i[k]) + f^T T_{i,j}(D_i[k]) \tag{3}$$

其中,f^E 和 f^T 表示两个成本因子,且 $f^E>0, f^T>0$.

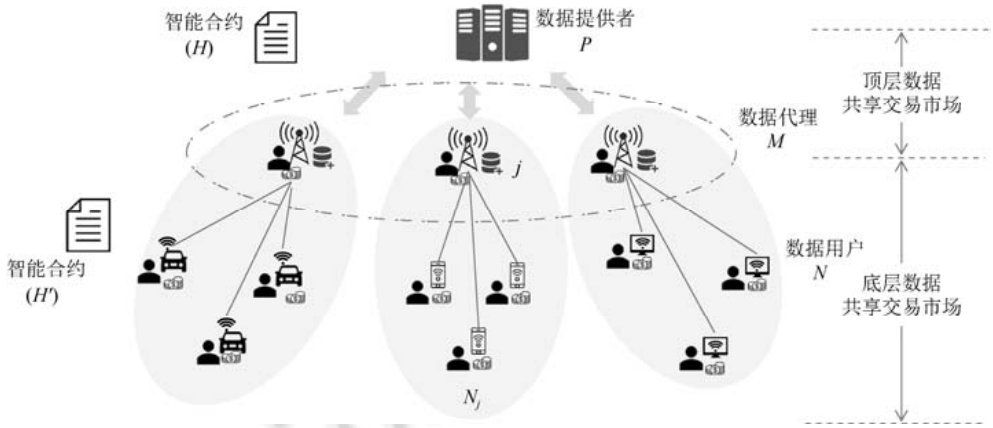


Fig.3 Hierarchical data sharing trading market based on blockchain

图 3 基于区块链的层次数据共享交易市场

3.2 问题形式化定义

假设 3 层数据交易市场的网络拓扑结构在拍卖过程中是固定的.也就是说,要求数据提供者、数据代理和数据用户在拍卖过程中不能改变它们当前所在的数据交易市场.由于共享参与主体的目标相互冲突,即数据提供者追求共享数据所得收益最大化,数据代理期望转卖数据所获的收益最大化,而数据用户则希望访问数据的成本最小化.在这种情况下,拍卖模型应该最大限度地解决数据共享中所有参与者的社会福利问题,实现有效的市场均衡.其目标函数是最大化数据用户对共享数据资源的效用和访问数据资源的传输成本之间的差值,形式化定义为

$$\left.\begin{aligned} SW(\mathbf{q}) = \max_{\mathbf{q}} \left\{ \sum_{i \in \mathcal{N}_j, j \in \mathcal{M}} \sum_{k=1}^{\mathbf{q}_i} \left(\mathbf{v}_i[k] - C_{i,j}(D_i[k]) - C_{j,\mathcal{P}}(D_i[k]) \right) \right\} \\ \text{s.t.} \sum_{i \in \mathcal{N}} \mathbf{q}_i = \mathcal{D} \end{aligned}\right\} \tag{4}$$

其中,$\mathbf{q}$ 表示 3 层数据交易市场中数据资源分配向量.$\mathbf{v}_i[k]$表示数据用户 $i \in \mathcal{N}$ 的效用向量 $\mathbf{v}_i$ 中的第 k 个元素,即 i 对第 k 个数据资源的效用.$C_{i,j}$ 为数据用户 i 通过数据代理 j 访问数据的传输成本,$C_{j,\mathcal{P}}$ 为数据代理 j 访问数据提供者 $\mathcal{P}$ 的数据资源的传输成本.$D_i[k]$表示数据用户 i 访问的第 k 个数据资源的大小.明显地,实现社会福利最大化即可得到最优的数据资源分配向量 $\mathbf{q}$.

为实现上述目标,需要提供数据共享参与者的个体效用和成本信息.然而,数据共享交易市场的层次化结构存在通信和服务等局限性,$\mathcal{P}$ 和 $\mathcal{M}$ 构成的顶层市场与 $\mathcal{M}$ 和 $\mathcal{N}$ 形成的底层市场之间的拍卖信息是不完全的.在顶层市场中,数据提供者无法直接获取到位于它的共享服务覆盖区域以外的底层市场中数据用户的数据需求.同样地,在底层市场中,数据代理能够供给数据用户的数据量在拍卖初始也不明确,因为在拍卖初始数据代理还没有获得数据提供者的数据报价.为此,本文提出一种层次数据拍卖机制以解决多层结构市场拍卖中信息不完全的社会福利最大化问题.

© 中国科学院软件研究所 http://www.jos.org.cn

3.3 层次数据拍卖机制

在本节中,首先将 SW 问题转化成层次数据交易市场中的最优数据分配问题.接下来给出层次数据拍卖机制的数学表达.最后,给出定理和证明.

定义 1(顶层市场的最优数据分配问题). 在顶层市场中,数据提供者将数据共享给数据代理.其最优数据分配问题是最大化数据代理对共享数据资源的效用与其访问数据的传输成本之间的差值.形式化定义为

$$\left.\begin{aligned}&\max_{\mathbf{q}^m}\sum_{j\in\mathcal{M}}\sum_{k=1}^{\mathbf{q}_j^m}\left(\mathbf{u}_j[k]-C_{j,\mathcal{P}}(D_j[k])\right)\\&\text{s.t.}\sum_{j\in\mathcal{M}}\mathbf{q}_j^m=\mathcal{D}\end{aligned}\right\}\tag{5}$$

其中,$\mathbf{q}^m$ 表示顶层市场中全体数据代理的数据分配向量,$\mathbf{q}_j^m$ 为数据提供者分配给数据代理 j 的数据量.$\mathbf{u}_j[k]$表示数据代理 j 对于第 k 个数据资源的效用,且 $\mathbf{u}_j[k]\in\mathbf{u}_j$.$D_j[k]$表示数据代理 j 访问的第 k 个数据资源的大小,$C_{j,\mathcal{P}}$ 为数据代理 j 访问数据提供者的数据资源的传输成本.

定义 2(底层市场的最优数据分配问题). 假设向量 $\mathbf{q}^{m*}$为顶层市场的最优数据分配解.在底层市场中,数据代理 j 将顶层市场所获得的数据资源 $\mathbf{q}^{m*}$转发给其分片 ACZ 内部数据用户.其最优数据分配问题是最大化数据用户对数据资源的效用与其访问数据资源的传输成本之间的差值.形式化定义为

$$\left.\begin{aligned}&\max_{\mathbf{q}_j^e}\sum_{i\in\{\mathcal{N}_j\}}\sum_{k=1}^{\mathbf{q}_j^e[i]}\left(\mathbf{v}_i[k]-C_{i,j}\left(D_i[k]\right)\right)\\&\text{s.t.}\sum_{i\in\{\mathcal{N}_j\}}\mathbf{q}_j^e[i]=\mathbf{q}_j^{m*},\ \sum_{j\in\mathcal{M}}\mathbf{q}_j^{m*}=\mathcal{D}\end{aligned}\right\}\tag{6}$$

其中,$\mathbf{q}_j^e$ 表示数据代理 j 所在分片 ACZ 中所有数据用户的数据分配向量,$\mathbf{q}_j^e[i]$ 为数据代理 j 分配给数据用户 i 的数据量.$\mathbf{v}_i[k]$表示数据用户 i 对于第 k 个数据资源的效用,且 $\mathbf{v}_i[k]\in\mathbf{v}_i$.$D_i[k]$表示数据用户 i 获得的第 k 个数据资源的大小,$C_{i,j}$ 表示数据用户 i 通过数据代理 j 访问数据资源的传输成本.

数据分配的流程描述如下:首先,数据提供者向数据代理 j 提供 $\mathbf{q}_j$ 单位的数据资源;然后,数据代理 j 将 $\mathbf{q}_j$ 转卖给其分片 ACZ 中的数据用户 $\mathcal{N}_j$. 如果分片 ACZ 这个底层子市场中的 $\mathcal{N}_j$ 数据需求等于数据代理 j 的数据供应 $\mathbf{q}_j$,则能够获得数据用户 $\mathcal{N}_j$ 的最优数据分配向量 $\mathbf{q}_j^{e*}$. 也就是说,当顶层市场和底层子市场的数据供需相等时,可以得到数据最优分配问题(5)和问题(6)的解向量 $\mathbf{q}^{m*}$和 $\mathbf{q}^{e*}$,并且等价于 **SW** 最大化问题(4).然而,受限于交易市场的层次结构,数据代理 $j\in\mathcal{M}$ 的效用向量 $\mathbf{u}_j$ 在拍卖初始时未知,故不能直接计算出 $\mathbf{q}^{m*}$和 $\mathbf{q}^{e*}$.在这种情况下,层次数据拍卖机制需要获取到完全信息来实现求解 **SW** 最大化问题.

本文提出在层次数据拍卖机制中引入同步机制,从而解决数据提供者通过 M 个数据代理向 N 个数据用户发送共享数据集 $\mathcal{D}$ 的社会福利最大化问题.具体方案描述如下:一方面,在顶层市场中采用 Ausubel 等人[39]提出的升序时钟拍卖与成交(ascending clock auction with clinching,简称 ACC)机制来解决数据最优分配问题(5).数据提供者在拍卖开始时将公布数据报价 p_0 给数据代理.在收到报价后,数据代理结合该报价下的效用提供对应的数据需求给数据提供者.然后,数据提供者则按照一个常数 C 的递增比例提高数据报价(即 p_0+C)并开始下一轮的拍卖.拍卖过程继续迭代,直到数据代理的数据需求等于数据提供者的共享数据资源集 $\mathcal{D}$;另一方面,在底层子市场中采用可扩展 ACC 机制来解决数据最优分配问题(6).每个数据代理能够提供给其分片 ACZ 内部数据用户的数据资源是其在顶层市场中拍卖所得.由于数据代理的效用不可预测,则要求数据代理将顶层市场的拍卖信息广播至其分片 ACZ.最后,为保证层次拍卖的同步,数据提供者需要制定数据交易分配规则和定价规则.

- 分配规则:数据代理在顶层市场中拍卖并获得的数据资源,必须即时地在其分片 ACZ 中进行再次拍卖;
- 定价规则:分片 ACZ 中数据资源的拍卖报价不得高于其在顶层市场中的最终拍卖价格.

下面,本文将给出层次数据拍卖机制的数学描述.假设数据提供者对于其共享数据资源集 $\mathcal{D}$ 的报价集为 $\mathbf{p}=\{p_0,p_1,\ldots,p_l\}$,$p_0$ 是初始拍卖价,p_l 是最终拍卖价.根据定理 1,顶层市场和其底层子市场共享数据集 $\mathcal{D}$ 的报价集

© 中国科学院软件研究所 http://www.jos.org.cn

是一样的,均为 $\mathbf{p}=\{p_0,p_1,\ldots,p_l\}$.

定理 1. 在层次数据拍卖机制中,顶层市场与底层子市场的数据拍卖行为同时终止.

证明:假设顶层市场中的数据报价集为 $\mathbf{p}_t=\{p_0,p_1,\ldots,p_l\}$,拍卖终止报价为 p_l;底层子市场中的数据报价集为 $\mathbf{p}_s=\{p_0,p_1,\ldots,p'_l\}$,拍卖终止报价为 p'_l,并且 $p_l\neq p'_l$.此时,假设 $p_l<p'_l$,意味着顶层市场的拍卖终止,但底层子市场仍在继续.那么,当终止报价为 p'_l 时,底层子市场中存在数据用户赢家拍卖到数据而其他用户放弃竞拍的情况.即在终止报价为 p'_l 时,必然存在数据用户改变其对于共享数据资源的需求情况.然而,在层次数据拍卖机制中规定:数据代理要首先收集其底层子市场中所有数据用户的共享数据需求,然后再决定自己的效用并向数据提供者提交对应的数据需求.这样,就会存在有数据代理在报价为 p'_l 时,在顶层市场中变更了其数据需求.那么,证明顶层市场的数据拍卖在报价为 p'_l 时并没有终止,显然与顶层市场中的拍卖终止报价为 p_l 的假设相矛盾.同理,若 $p_l>p'_l$,则底层子市场中的数据用户将无法变更其数据需求.相应地,数据代理也不会改变其数据需求.因此,$p_l>p'_l$ 不会成立.综上所述,数据拍卖在顶层市场与底层子市场会同时终止. □

当数据报价为 $p_t\in\mathbf{p}$ 时,数据代理 j 的数据需求表示为

$$\mathbf{r}_j^m(p_t)=\sum_{i\in\mathcal{N}_j}\mathbf{r}_j^e(p_t)[i]-C_{j,\mathcal{P}} \tag{7}$$

其中,$C_{j,\mathcal{P}}$ 为数据代理 j 访问数据提供者的数据资源的传输成本.$\mathbf{r}_j^e(p_t)$ 表示数据代理 j 所在的分片 ACZ 中数据用户 $\mathcal{N}_j$ 对于报价 p_t 的数据需求向量,$\mathbf{r}_j^e(p_t)[i]$ 为分片 ACZ 数据用户 $i(i\in\mathcal{N}_j)$对于报价 p_t 的数据需求.

当数据报价为 $p_t\in\mathbf{p}$ 时,数据用户 i 的数据需求表示为

$$\mathbf{r}_j^e(p_t)[i]=\sum_{k\in\mathbf{v}_i}I(k-C_{i,j},p_t) \tag{8}$$

其中,$C_{i,j}$ 为数据用户 i 通过数据代理 j 访问数据的传输成本.$I(x,y)$代表指示函数,当 $x\leqslant y$ 时,$I(x,y)=0$;当 $x>y$ 时,$I(x,y)=1$.因此,数据用户 i 对于报价 p_t 的数据需求 $\mathbf{r}_j^e(p_t)[i]$ 是随着报价 p_t 的增加而递减的,且对于任意 $k\in\mathbf{v}_i$,如果 $y'>y$ 且 $\{y,y'\}\in\mathbf{p}$,那么,$I(k,y')\leqslant I(k,y)$.

假设数据代理 j 在报价为 $p\in\mathbf{p}$ 时将其在顶层市场拍卖得到的第 k 个数据资源转卖给数据用户 i,则对于第 k 个数据资源的效用表示为 $\mathbf{u}_j[k]=p-C_{i,j}(D_j[\mathrm{k}])$,其中,$\mathbf{u}_j[k]$是数据代理 j 的效用向量中的第 k 个元素,$C_{i,j}$ 为访问数据资源的传输成本.根据分配规则,当数据报价为 $p_t\in\mathbf{p}$ 时,数据代理 j 和数据用户 $i\in\mathcal{N}_j$ 拍卖所得数据的总量分别为

$$\mathbf{q}_j^m(p_t)=\max\left\{0,\mathcal{D}-\sum\nolimits_{k\in\mathcal{M}\setminus j}\mathbf{r}_k^m(p_t)\right\} \tag{9}$$

$$\mathbf{q}_i^e(p_t)=\max\left\{0,\mathbf{q}_j^m(p_t)-\sum\nolimits_{k\in\mathcal{N}_j\setminus i}\mathbf{r}_j^e(p_t)[k]\right\} \tag{10}$$

当 $p_t=p_l$ 时拍卖结束,即可得到数据最优分配问题(5)和问题(6)的解向量 $\mathbf{q}^{m*}$和 $\mathbf{q}^{e*}$.并且,上述两个公式(9)和公式(10)可进一步表示为

$$Q_j^m(p_t)=\begin{cases}\max\left\{0,\mathbf{q}_j^m(p_t)\right\},(t=0)\\ \max\left\{0,\mathbf{q}_j^m(p_t)-\mathbf{q}_j^m(p_{t-1})\right\},\left(t\in\{1,2,\ldots,l\}\right)\end{cases} \tag{11}$$

$$Q_i^e(p_t)=\begin{cases}\max\left\{0,\mathbf{q}_i^e(p_t)\right\},(t=0)\\ \max\left\{0,\mathbf{q}_i^e(p_t)-\mathbf{q}_i^e(p_{t-1})\right\},\left(t\in\{1,2,\ldots,l\}\right)\end{cases} \tag{12}$$

只要数据代理或者数据用户在数据报价为 $p_t\in\mathbf{p}$ 时能够获得共享数据资源,交易就可以发生.并且,该数据代理或数据用户需要为每单位数据资源支付价格 p_t.根据支付规则,数据代理 j 和数据用户 $i\in\mathcal{N}_j$ 需要支付的价格表示为

$$P_j^m(\mathbf{p},\mathbf{Q}^m)=\sum_{t=0}^{t=l}\sum_{k=1}^{k=Q_j^m(p_t)}(p_t-C_{j,\mathcal{P}}(D_j[k])) \tag{13}$$

© 中国科学院软件研究所 http://www.jos.org.cn

$$P_i^e(\mathbf{p},\mathbf{Q}^e)=\sum_{t=0}^{t=l}\sum_{k=1}^{k=Q_i^e(p_t)}(p_t-C_{i,j}(D_i[k]))\tag{14}$$

其中,$C_{j,p}$ 为数据代理 j 访问数据提供者的共享数据资源所需传输成本,$C_{i,j}$ 为数据用户 i 通过数据代理 j 访问数据资源所需传输成本.$D_j[k]$为数据代理 j 拍卖所获得的数据提供者的第 k 个数据资源大小,$D_i[k]$为数据用户 i 通过数据代理 j 拍卖所获得的第 k 个数据资源大小.

3.4 基于智能合约的3层数据拍卖算法

在 3 层数据拍卖机制中,数据提供者可以在拍卖过程中逐步获取底层数据用户对于共享数据资源的需求信息,而数据用户也可以在这个过程中逐步获得数据代理提供的共享数据信息.这样,拍卖结束时即得到最优数据分配问题的最优解 $\mathbf{q}^{m*}$和 $\mathbf{q}^{e*}$,实现社会福利最大化.算法 1 给出了基于智能合约的 3 层数据拍卖算法的过程描述,具体步骤如下.

① 拍卖智能合约 $\mathcal{H}$ 在区块链系统初始化阶段被编译和部署.数据提供者 $\mathcal{P}$ 调用智能合约 $\mathcal{H}$ 中的 **Register** 接口注册并初始化顶层数据交易市场,提供相关投标数据,如:共享数据资源集 $\mathcal{D}$ 的数量 D、初始报价 p 和拍卖迭代过程中每一轮的价格增量 C.同样地,拥有账户储备资金的数据代理 j 通过 **Register** 接口注册加入顶层市场,并初始化其数据需求 $\mathbf{r}_j^m\leftarrow 0$; ② 数据代理 j 调用智能合约 $\mathcal{H}$ 的 **Create** 接口创建它所连接的底层子市场的拍卖智能合约 $\mathcal{H}_j$. 随后,其分片 ACZ 中拥有储备资金的数据用户都可以通过调用智能合约 $\mathcal{H}_j$ 的 **Register** 接口加入底层子市场,并初始化其数据需求 $\mathbf{r}_j^e\leftarrow[0,...,0]$; ③ 根据初始报价 p,底层子市场的数据用户通过智能合约 $\mathcal{H}_j$ 的 **UpdateDemand** 接口更新其数据需求 $\mathbf{r}_j^e[i]$. 结合数据用户的需求更新,数据代理通过智能合约 $\mathcal{H}$ 的 **UpdateDemand** 接口更新其数据需求 $\mathbf{r}_j^m$; ④ 数据提供者 $\mathcal{P}$ 按照公式(9)共享对应数量的数据资源给数据代理,数据代理依据公式(10)分配相应的数据资源给数据用户;⑤ 根据公式(9)和公式(10),数据代理和数据用户分别调用智能合约 $\mathcal{H}$ 和 $\mathcal{H}_j$ 的 **Pay** 接口完成支付;⑥ 如果顶层市场和底层市场的供需不相等,则需要继续进行下一次拍卖.由数据提供者 $\mathcal{P}$ 调用智能合约 $\mathcal{H}$ 的 **UpdatePrice** 接口更新报价 $p\leftarrow p+C$, 然后从算法 1 的步骤 3 开始下一轮迭代;⑦ 整个数据拍卖结束后,数据代理和数据用户可以调用对应的智能合约的 **Withdraw** 接口取回各自账户的剩余资金.

算法 1. 基于智能合约的 3 层数据拍卖算法.

输入: D, $p\leftarrow p_0$, C=1, $\mathbf{r}_j^m\leftarrow 0$, $\mathbf{r}_j^e\leftarrow[0,...,0]$;

输出:$\mathbf{q}^{m*}$,$\mathbf{q}^{e*}$,$\mathbf{p}^m$,$\mathbf{p}^e$.

1. 在顶层市场中,数据提供者 $\mathcal{P}$ 通过智能合约 $\mathcal{H}$ 的 **Register** 接口注册数据资源服务;
2. 设置 $\mathcal{H}$ 中的全局变量,包括:拍卖数据资源集的数量 D,数据初始报价 $p\leftarrow p_0$,每轮价格增量 C=1;
3. **for** $j\in\mathcal{M}$ **do**
4. 拥有账户储备资金的数据代理 j 通过智能合约 $\mathcal{H}$ 的 **Register** 接口参与顶层市场拍卖;
5. 数据代理 j 通过智能合约 $\mathcal{H}$ 的 **Create** 接口创建一个智能子合约 $\mathcal{H}_j$, 管理其底层子市场交易;
6. **for** $i\in\mathcal{N}_j$ **do**
7. 拥有账户储备资金的数据用户 i 通过智能子合约 $\mathcal{H}_j$ 的 **Register** 接口注册并参与到其数据代理 j 所连接的底层子市场拍卖中;
8. **end for**
9. 设置 $\mathcal{H}_j$ 中的全局变量,包括:数据代理 j 对于数据资源的需求 $\mathbf{r}_j^m\leftarrow 0$, 数据用户 $i\in\mathcal{N}_j$ 对于共享数据资源的需求 $\mathbf{r}_j^e\leftarrow[0,...,0]$;
10. **end for**
11. **while** $D\neq\sum_{j\in\mathcal{M}}\mathbf{r}_j^m$ **do**

© 中国科学院软件研究所 http://www.jos.org.cn

12. **for** $j \in \mathcal{M}$ **do**
13. **for** $i \in \mathcal{N}_j$ **do**
14. 数据用户 i 调用智能子合约 $\mathcal{H}_j$ 的 **UpdateDemand** 接口,更新其数据资源需求 $\mathbf{r}_j^e[i]$;
15. **end for**
16. 数据代理 j 调用智能合约 $\mathcal{H}$ 的 **UpdateDemand** 接口,更新其数据资源需求 $\mathbf{r}_j^m$;
17. **end for**
18. 数据提供者 $\mathcal{P}$ 按照公式(9)将对应数量的数据资源提供给数据代理,数据代理 j 则按照公式(10)将对应数量的数据资源提供给它所在分片 ACZ 中的数据用户 $\mathcal{N}_j$;
19. 根据公式(13)和公式(14),数据代理 j 和数据用户 $\mathcal{N}_j$ 将分别通过智能合约 $\mathcal{H}$ 和 $\mathcal{H}_j$ 的 **Pay** 接口完成其拍卖所得数据资源的支付;
20. 数据提供者 $\mathcal{P}$ 调用智能合约 $\mathcal{H}$ 的 **UpdatePrice** 接口,更新数据报价 $p \leftarrow p + C$;
21. **end while**
22. 拍卖结束后,数据代理 j 和数据用户 $\mathcal{N}_j$ 可以通过分别调用智能合约 $\mathcal{H}$ 和 $\mathcal{H}_j$ 的 **Withdraw** 接口取回自己账户剩余的储备资金.

3.5 算法定理

本文提出的层次数据拍卖算法具有一定的高效率和实用性.为证明这些属性,本文考虑与经典的基于 ACC 的双向拍卖算法[41]进行对比.双向拍卖[31]是一种广泛应用于现实交易中的实用拍卖模式,其中,交易双方分别向拍卖中间方提交要价和出价,最后由拍卖中间方匹配双方投标价格并确定相应的资源分配和定价规则.然而,标准的拍卖算法在投标者具有多单位商品需求时往往效率偏低.基于 ACC 的双向拍卖算法引入了 ACC 这种同类商品上升竞价拍卖机制,能够很好地应对效率问题,获得高效、实用的拍卖模型.因此,选取它作为基准算法以证明本文算法的有效性.下面,我们给出算法定理的证明过程.

定理 2. 在不考虑 ShareBC 通信和共享服务的局限性以及访问共享数据所需要的传输成本时,本文提出的层次数据拍卖机制与基于 ACC 的双向拍卖机制是等价的.

证明:假设数据提供者将对 D 个单位的数据资源进行共享交易.首先,分析采用基于 ACC 的双向拍卖机制,即物联网数据用户直接与数据提供者进行数据交易.用 $\mathbf{Q}_i$ 表示数据用户 $i \in \mathcal{N}$ 的数据分配向量,数据拍卖报价为 $\mathbf{p}=\{p_0,p_1,\ldots,p_f\}$,$\mathbf{r}(p_d)[\boldsymbol{i}]$表示拍卖报价为 $p_d \in \mathbf{p}$ 时,数据用户 i 对于共享数据资源的需求.假设 $p_d \in \mathbf{p}$ 是数据用户 i 获得第 1 份共享数据资源的价格,之后,每次的拍卖报价为 $p_d \leftarrow p_d+C$,满足:

$$1 = Q_i(p_d) = D - \sum_{k \in \mathcal{N} \setminus i} \mathbf{r}(p_d)[k],\ \sum_{i \in \mathcal{N}} \sum_{k=p_0}^{p_d - C} Q_i(k) = 0, (p_d > 0) \tag{15}$$

根据公式(15),可以推出:

$$D - \sum_{k \in \mathcal{N}} \mathbf{r}(p_d)[k] + Q_i(p_d) = 1 \tag{16}$$

接下来,采用本文提出的层次数据拍卖机制进行分析.假设在 3 层共享数据交易市场存在 2 个数据代理 M_1、M_2,其中,M_1 连接的底层子市场中有 i 个数据用户.M_1 和 M_2 的数据分配向量为 $\mathbf{Q}_1^m$ 和 $\mathbf{Q}_2^m$,数据拍卖报价为 $\mathbf{p}=\{p_0, p_1,\ldots,p_f\}$.当拍卖报价为 $p_t \in \mathbf{p}$ 时,M_1 和 M_2 所能获得的数据量为

$$\left.\begin{aligned} Q_1^m(p_t) &= \max\left\{0, D - \mathbf{r}_2^m(p_t)\right\}, \\ Q_2^m(p_t) &= \max\left\{0, D - \mathbf{r}_1^m(p_t)\right\} \end{aligned}\right\} \tag{17}$$

其中,$\mathbf{r}_j^m$ 为数据代理 $j \in \{1,2\}$ 的共享数据资源需求.假设 $\mathbf{Q}_i^e$ 为数据用户 $i \in M_1$ 的数据分配向量,$p_h \in \mathbf{p}$ 为底层子市场数据用户 i 第 1 次在拍卖中获得数据的价格,之后,每次的拍卖报价为 $p_h \leftarrow p_h+C$,则有:

© 中国科学院软件研究所 http://www.jos.org.cn

$$1=Q_i^e(p_h)=Q_1^m(p_h)-\sum_{k\in\mathcal{N}_1\setminus i}\mathbf{r}_1^e(p_h)[k],\ \sum_{i\in\mathcal{N}_1}\sum_{k=p_0}^{p_h-C}Q_i^e(k)=0,\ (p_h>0) \tag{18}$$

其中,$\mathbf{r}_1^{p_h}[i]$是数据用户 i 在价格 $p_h\in\mathbf{p}$ 下的共享数据资源需求.根据公式(18),可以推出:

$$Q_1^m(p_h)-\sum_{k\in\mathcal{N}_1}\mathbf{r}_1^e(p_h)[i]+Q_i^e(p_h)=1 \tag{19}$$

根据公式(17)和公式(19),计算如下:

$$\begin{aligned}1&=D-\mathbf{r}_2^m(p_h)-\sum_{i\in\mathcal{N}_1}\mathbf{r}_1^e(p_h)[i]+Q_i^e(p_h)\\&=D-\mathbf{r}_2^m(p_h)-\mathbf{r}_1^m(p_h)+Q_i^e(p_h)\\&=D-\sum_{i\in\mathcal{N}}\mathbf{r}^e(p_h)[i]+Q_i^e(p_h)\end{aligned} \tag{20}$$

比较公式(16)和公式(20),不难得出 $p_d=p_h$.因此,在不考虑 ShareBC 通信和服务限制以及访问共享数据资源所产生的传输成本的情况下,本文的层次数据拍卖机制与基于 ACC 的双向拍卖机制是等价的. □

4 性能评估

4.1 分片协议比较与分析

本节主要从分片形成、分片内部共识以及安全性和可扩展性等方面评估 ShareBC 框架分片协议.表 1 提供了与当前经典区块链分片协议的全面比较.本文第 2.2 节在基于 ShareBC 实现的数据共享关键步骤中针对分片协议,如分片构建和共识过程进行了阐述,下面就分片设置与对比分析展开描述.

Table 1 Sharding settings and performance comparisons

表 1 分片设置及其性能对比

协议	节点加入	交易模型	协议强一致性	节点分配	分片内共识			安全性(恶意节点容忍比例)	扩展性
					节点配置	Leader	通信复杂性		
RSCoin[42]	基于许可的	UTXO	✓	×	静态	内部选举	O(n)	1/3	2 000 tx/sec
Chainspace[43]	灵活	账户/余额	✓	×	灵活	内部选举	O(n^2)	1/3	350 tx/sec
Elastico[44]	PoW	UTXO	✓	动态随机	周期变换(完全交换)	内部选举	O(n^2)	1/3	16 blocks/110 sec
OmniLedger[45]	PoW/PoS	UTXO	✓	动态随机	周期变换(替换子集)	内部选举	O(n)	1/4	6 000 tx/sec
RapidChain[46]	线下 PoW	UTXO	✓	动态随机	周期变换	内部选举	O(n)	1/3	7 300 tx/sec
Monoxide[47]	PoW	账户/余额	✓	静态	静态	×	×	1/2	11 694 tx/sec
ShareBC	基于许可的	账户/余额	✓	静态	周期变换	内部选举	O(n)	1/3	✓

✓:具有该属性;×:不具有该属性

在协议设置方面,节点加入表示允许节点加入当前 epoch 所依据的规则和标准.例如,基于 PoW 或 PoS 机制获得身份资格,这对于非许可区块链系统是阻止女巫攻击的重要方法.然而,本文提出的 ShareBC 基于许可链,允许系统在假定相对信任的环境中运行,其中注册成功的物联网设备将准予参与节点资格.此外,ShareBC 采用账户/余额交易模型,这是因为该模型简单且更适用于智能合约,支持具有任意金额的交易通过一个发送账户和一个接收账户执行交易而无需双边多个 UTXOs,这种平衡性可以扩展到更为复杂的状态,从而支持可编程的应用程序逻辑.最后,ShareBC 分片方案采用经典的拜占庭容错协议在协商的共识方面具有强一致性.

节点分配是指参与节点如何分配到对应的区块链系统分片中.现有的多数工作是根据 epoch 产生的随机数即基于可公开验证的随机性进行分配,少数研究,如 Monoxide[47]协议节点分配不是随机的而是基于地址进行划分的.在 ShareBC 分片协议中,对于每个成功注册身份的物联网设备,系统会根据某个关键特征值(如地理坐标范围)将设备分配到对应的 ACZ 中.在分片内共识方面,通常其节点配置可以是静态(永久性)或者动态周期性变化的,如轮流替换、完全交换或更换子集节点.考虑到物联网设备的移动性和 ACZ 安全性,ShareBC 会设置定期变

© 中国科学院软件研究所 http://www.jos.org.cn

换 ACZ 内的设备节点.并且,每个 ACZ 会在每个 epoch 内进行 leader 选举,leader 则来自于分片内部的物联网设备节点.通信复杂性表明分片内部节点间的通信时间复杂度,假设表示 ACZ 内节点的数量,那么 ShareBC 中每个 ACZ 内部的通信复杂性为 O(n).

在安全性和可扩展性方面,ShareBC 对手模型是基于 BFT 设置的,其协商一致性协议可以容忍的恶意或者错误节点数量小于 1/3.表 1 中显示的吞吐量数值与测试实验参数设置相关[45].其中,RSCoin 实验参数包括 3 个节点/分片和 10 个分片;ChainSpace 实验参数包括 4 个节点/分片和 15 个分片;Elastico 实验参数包括 100 个节点/分片和 16 个分片;OmniLedger 实验参数包括 72 个节点/分片(12.5%对手)和 25 个分片;RapidChain 实验参数包括 250 个节点/分片和 4 000 个节点数量;Monoxide 包括 2 048 个分片和 48 000 个节点数量.吞吐量数值表明,这些分片系统都具有可扩展性.ShareBC 分片协议需要经过两轮验证,由物联网设备节点(follower)首先通过 PBFT 共识验证 ACZ 分片内部的一致性,然后提交给联盟链委员会验证全局一致性并添加验证成功的区块上链,本文方案降低了交易延迟并有效提高了交易吞吐量,因为上链区块不需要类似 Bitcoin 网络中需要等待 6 个区块的确认时间.此外,本文共识机制在一定程度上受到 RSCoin 的启发,ShareBC 系统中 Committee 依赖分布式分片 ACZ,并同时保持了对于数据共享交易的完全控制,因而具有强大的透明度和可审计性安全保证.

4.2 原型实现

智能合约实现了以不可否认性和自动化的方式强制执行激励机制中的关键事件,提高了数据共享安全和效率.本实验针对拍卖智能合约 $\mathcal{H}$ 和其子合约 $\mathcal{H}_j$ 的性能测试开发了一个原型系统,并将其部署到 Ethereum 测试网络中以计算智能合约和各个接口的 Gas 成本.在 Ethereum 区块链中,Gas 价格代表了执行某个任务所消耗的 Ether,其测量单位为 Wei 且 1 Wei=10^{-18}Ether.表 2 中显示了拍卖智能合约 $\mathcal{H}$ 和 $\mathcal{H}_j$ 中各个接口的 Gas 成本均值(20 轮测试).其中,执行成本代表智能合约执行指令的 Gas 消耗;其他成本则表示调用接口的交易所消耗掉的 Gas.根据表 2 所示测试结果,整个智能合约中 Gas 消耗最大的是 Create 接口,但其只是在某个数据代理创建它所连接的底层子市场时才被调用 1 次.

Table 2 The Gas cost of interfaces in the smart contracts $\mathcal{H}$ and $\mathcal{H}_j$

表 2 智能合约 $\mathcal{H}$ 和 $\mathcal{H}_j$ 接口的 Gas 成本

接口	执行成本(Gas)	其他成本(Gas)	交易成本(Gas)	总成本($)
Create	1 120 572	382 327	1 502 899	0.715 379 92
Register($\mathcal{H}$)	652 320	21 191	673 511	0.320 591 24
Register($\mathcal{H}_j$)	60 978	21 191	82 169	0.039 112 44
UpdateDemand	20 671	21 442	42 113	0.020 045 79
UpdatePrice	5 565	21 442	27 007	0.012 855 33
Pay	27 260	21 191	48 451	0.023 062 68
Withdraw	12 884	5 799	18 683	0.008 893 11

假设在一个层次数据拍卖系统中存在 1 个数据提供者、2 个数据代理和 10 个数据用户.根据当前汇率 1 Ether≈238$且 1 Gas=0.000000002 Ether 进行计算,该系统中数据提供者在区块链网络中发布一个共享数据交易仅需要 0.320 591 24$的成本;每个底层子市场中数据需求者(包括 1 个数据代理和 5 个数据用户)历经一轮数据拍卖的总成本为 1.490 184$,平均每个数据需求者需要花费的成本为 0.248 364$.注意,这里计算的一轮数据拍卖具体包括调用 1 次 Register($\mathcal{H}$)、1 次 Create、5 次 Register($\mathcal{H}_j$)、6 次 UpdateDemand 和 6 次 Pay 接口.经过反复测试,结果表明,执行智能合约 $\mathcal{H}$ 和 $\mathcal{H}_j$ 的成本开销较低,说明基于智能合约实现的层次拍卖机制应用于物联网数据激励共享框架中是经济可行的.

4.3 仿真结果与分析

通过仿真模拟对本文所提出的层次数据拍卖算法进行了性能测试.实验假设数据共享参与者的规模为 $(x,y,(z_1,z_2,\ldots,z_y))$,其中,$x$ 表示数据提供者的数量,y 表示数据代理的数量,z_i 表示其所在分片 ACZ 中的数据用户的

© 中国科学院软件研究所 http://www.jos.org.cn

数量.仿真参数设置如下:考虑 3 组参与者规模分别为#1:(1,3,(5,5,5))、#2:(1,3,(10,10,10))和#3:(1,3,(15,15,15)).

在顶层市场中,数据提供者拥有的共享数据资源数量为D=50;在底层市场中,数据用户 $i\in\mathcal{N}_j$ 的传输功率为 P_i=2W,通信带宽 B=10MHz,数据用户(或数据代理) $i\in\mathcal{N}\cup\mathcal{M}$ 与数据代理(或数据提供者) $j\in\mathcal{M}\cup\mathcal{P}$ 之间的距离 $d_{i,j}$ 分布范围是[0,20].成本因子 f^E 的取值范围为[0,1],且 f^E=1–f^E.数据用户所访问的数据资源大小为 1.数据用户 $i\in\mathcal{N}_j$ 的效用向量 $\mathbf{v}_i$ 对应的元素大小分布是[0,100].参考 Hong 等人的工作[9],假设单位距离 $d_{i,j}$=1m 的噪声功率和信道功率分别为δ^2=–120dBm 和β_0=–50dB,那么,数据用户 $i\in\mathcal{N}_j$ 和数据代理 j 之间的信道容量计算为 $H_{i,j}=B\log_2(1+\lambda_i^0/d_{i,j}^2)$,其中,$\lambda_i^0$ 表示数据用户 i 在 $d_{i,j}$=1m 时的接收信噪比,且 $\lambda_i^0=\beta_0P_i/\delta^2$.最后,为确保实验结果的准确性,每个实验数据均取自于 100 个独立仿真结果的均值.

为了验证算法的有效性,实验在参与者规模分别为#1、#2 和#3 时对社会福利进行了测试.图 4 显示了层次数据拍卖算法在不同规模下社会福利函数的收敛性.如图 4 所示,本文算法在不同数据共享规模下都能够快速地获得最大的社会福利.并且,随着参与者规模(x,y,(z_1,z_2,…,z_y))的扩大,收敛后的社会福利值也越来越大.这是因为,3 层数据交易市场的资源竞争力会随着数据共享用户数量的增加而增大,同时也意味着数据用户需要支付更高的价格才能成为拍卖赢家并访问数据.

图 5 描述了数据需求者(包括数据代理和数据用户)的总需求与数据提供者的供应之间的关系.整体趋势表明,数据提供者的数据供给随着数据拍卖价格的提高不断增加,而数据代理和数据用户的总需求会随着数据拍卖报价的提高而持续下降.最终,两者曲线会收敛到同一个值,即数据提供者拥有的共享数据资源数量 D=50.结合图 4 和图 5 可知,当数据代理和数据用户对于共享数据的总需求等于数据提供者的供应时,即实现了社会福利的最大化.此外,图 4 所示的社会福利曲线和图 5 所示的数据提供者的供应曲线变化趋势相同,原因是:只有在数据提供者愿意共享的数据资源数量发生改变时,社会福利才会变化.实验结果表明,层次数据拍卖机制是有效的,能够实现社会福利的最大化.

图 6 展示了算法在参与者规模为#2 时传输成本对于社会福利的影响.从图中可以看出,成本因子 f_E 越小,社会福利函数收敛值越大,即传输成本的增加会导致最大社会福利的下降.而且在收敛前,成本因子 f_E 越大的社会福利曲线变化越快,对应在拍卖系统中的数据用户就会更快地获得到数据资源.这种情况发生的原因是,在层次数据拍卖机制中,底层子市场的传输成本是分片 ACZ 内部数据用户的开销成本.在对于共享数据资源效用相同的前提下,传输成本越高,数据用户参与拍卖的价格自然就会越低.考虑在相同的市场竞争力下,拍卖报价越低,成交价格越低,赢家竞拍到数据资源的时间越早.

图 7 分别描述了在#1、#2 和#3 这 3 种参与者规模下的数据提供者、数据代理和数据用户在实现社会福利最大化后的总效用.如图所示,每组柱状条中的左 1 为数据提供者的净效用,左 2 与左 1 的差值为数据代理的净效用,左 3 与左 2 的差值为数据用户的净效用.明显地,数据提供者、数据代理和数据用户的净效用均为正,说明提出的层次数据拍卖机制满足弱预算平衡性.

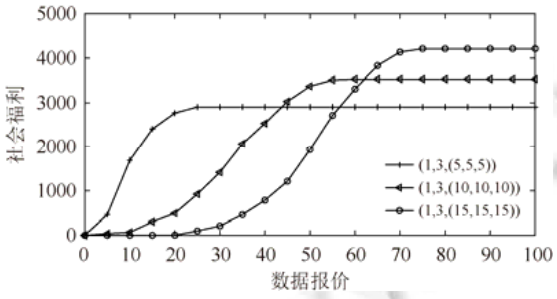


Fig.4 Convergence of social welfare functions
图 4 社会福利函数的收敛性

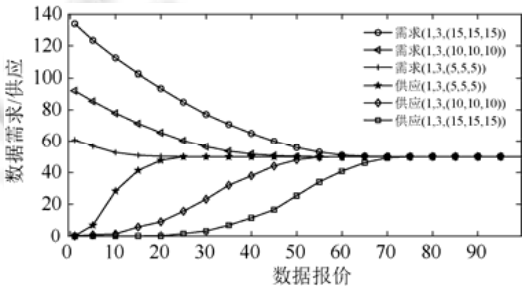


Fig.5 Relationship between demands and supplies
图 5 数据总需求与总供应之间的关系

© 中国科学院软件研究所 http://www.jos.org.cn

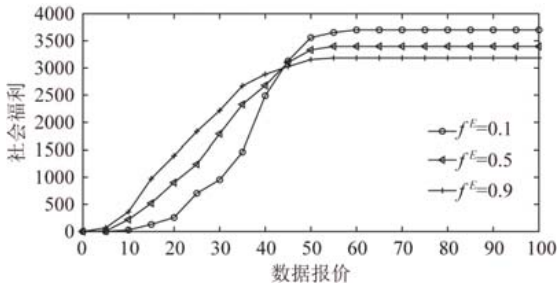


Fig.6 Social welfare under different cost factors
图 6 不同成本因子下的社会福利

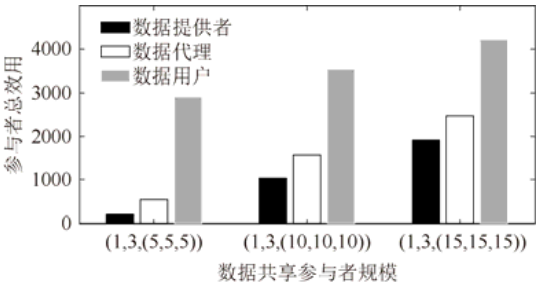


Fig.7 Overall utility of data sharing participants
图 7 数据共享参与者各自总效用

在层次数据拍卖机制中,要求数据代理在顶层市场中拍卖获得共享数据资源之后,立即在其底层子市场中向数据用户进行转卖.实验针对层次数据拍卖机制的实时性展开了如图 8 和图 9 所示的测试.

在图 8 中,描述了 3 层数据拍卖算法减少的数据交易延时随需求者(数据代理和数据用户)数量发生变化的情况.结论是,减少时延会随着共享用户数量的增加而减少.

图 9 解释了这种趋势的原因.在图 9 中,分别展示了在#1、#2 和#3 参与者规模下的数据代理和数据用户的整个拍卖过程.其中,$x_i(i\in\{1,2,3\})$表示数据用户从拍卖赢得第 1 个共享数据资源集到拍卖结束的过程.由于$x_1>x_2>x_3$,说明参与者的规模越小,数据用户越少,拍卖结束越快,数据资源也能更快获得.这个不难理解,数据共享交易的参与者规模决定了市场竞争力的大小,当市场竞争力较小时,数据用户赢得共享数据资源的时间较短.因此,当物联网中参与数据共享的设备数量较少时,算法的实时性会更明显.

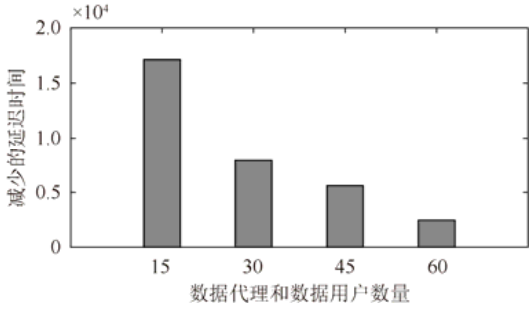


Fig.8 Reduction in latency with the number of demanders
图 8 减少时延随需求者数量的变化

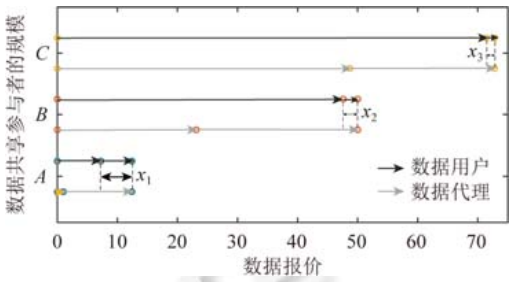


Fig.9 Auction process of players in different cases
图 9 数据用户/代理在不同规模下的拍卖过程

最后,在不同数量的数据用户设置下,实验针对最大社会福利进行了算法对比测试.其中,测试算法包括基于 ACC 的双向拍卖算法和基于智能合约的 3 层数据拍卖算法.实验结果表明,两种拍卖算法能够实现的最大社会福利基本是相同的.

图 10 所示的微小差距可能是由于两者在实验中的取值皆为均值所造成的.实验结果验证了定理 2 的正确性.即,在不考虑 ShareBC 通信和服务局限性以及访问共享数据所需要的传输成本时,本文提出的层次数据拍卖机制与基于 ACC 的双向拍卖机制等价.

图 11 展示了算法扩大节点规模后的测试效果,随着 ACZ 组数以及每个分片 ACZ 中的数据用户数量的增加,算法执行所需要的迭代轮次也逐渐增加,从图中可以看出,本文算法呈线性增长趋势其扩展性表现良好.

© 中国科学院软件研究所 http://www.jos.org.cn

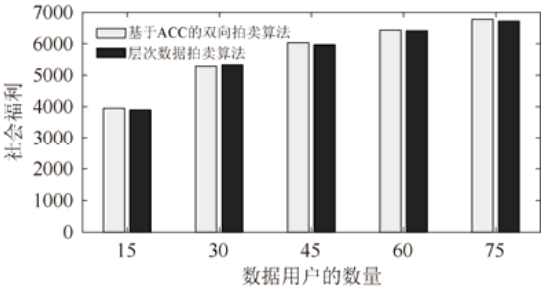


Fig.10 Average maximum social welfare in hierarchical data auction and double auction algorithms

图 10 层次数据拍卖算法和基于 ACC 的双向拍卖算法的最大社会福利

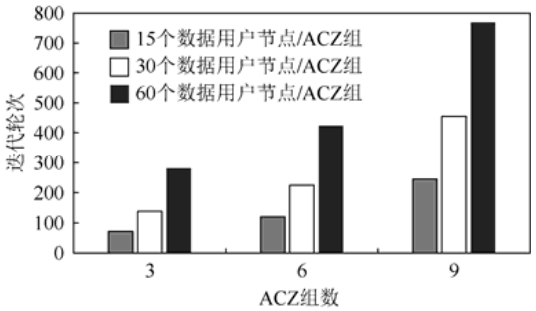


Fig.11 Average number of rounds with varying ACZ groups and number of data users in each ACZ

图 11 ACZ 组数和每个 ACZ 中数据用户节点数量对迭代轮次的影响

5 总结与展望

本文研究了基于区块链的高效物联网数据激励共享方案.一方面,该方案提出了一个高效的区块链物联网数据激励共享框架(称为 ShareBC).为了提升系统的数据共享交易处理能力,ShareBC 引入分片技术将网络中物联网设备划分成若干分片异步共识区,将原来需要全网节点共同进行的交易验证工作在分片异步共识区并行处理.在此基础上,为 ShareBC 设计了高效的共识机制,这种共识机制具有强大的透明度和可审计性保证,并且在计算成本和可扩展性方面也具有优势;另一方面,该方案提出了基于层次数据拍卖模型的激励机制,解决了数据提供者与数据需求者之间的共享数据资源分配问题,其中无法访问共享资源的数据用户可以通过数据代理帮助其获取数据,以鼓励更多的物联网用户加入到数据共享中.在层次数据拍卖机制中,设计了包括数据代理在内的 3 层数据拍卖模型和相关的数据分配以及定价规则,并考虑了传输数据成本对于社会福利的影响.最后,为确保拍卖机制的不可否认性和执行效率,利用智能合约部署的形式使其自动生效.理论证明和实验评估表明,本文所提出的激励共享方案具有个体理性、激励兼容性、弱预算平衡和实时性以及可扩展性的特点,并且具有较低的计算成本和良好的实用性.

未来工作将继续探索区块链技术在物联网领域的数据共享应用.为了解决区块链固有的性能瓶颈问题,需要针对系统扩展性进行提升研究(如:分片、链下支付通道).目前,ShareBC 链尚未实现,本文给出了 ShareBC 分片协议的设置建议和性能对比分析,后面将继续研究 ShareBC 分片协议的具体实现,考虑在动态物联网环境中如何形成分片和进行分片的动态调整并且能够同时平衡分散性、安全性以及可扩展性.此外,多链驱动的异构物联网共享应用平台也可进一步提高区块链系统性能.在本文模型中,ShareBC 是基于许可链来设置的,数据共享交易在假设相对信任的环境中进行,所有参与节点,如数据提供者,均具有经联盟组织策略授权的成员资格.在下一步工作中,可以考虑在激励机制中设置信用评价和奖惩机制以提升共享数据质量和交易安全性.

References:

[1] Tan HB, Zhou T, Zhao H, Zhao Z, Wang WD, Zhang ZX, Sheng NZ, Li XF. Archival data protection and sharing method based on blockchain. Ruan Jian Xue Bao/Journal of Software, 2019,30(9):2620–2635 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5770.htm [doi: 10.13328/j.cnki.jos.005770]

[2] Yao HP, Mai TL, Wang JJ, Ji Z, Jiang CX, Qian Y. Resource Trading in blockchain-based industrial Internet of Things. IEEE Trans. on Industrial Informatics, 2019,15(6):3602–3609. [doi: 10.1109/TII.2019.2902563]

[3] Liu AD, Du XH, Wang N, Li SZ. Blockchain-based access control mechanism for big data. Ruan Jian Xue Bao/Journal of Software, 2019,30(9):2636–2654 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5771.htm [doi: 10.13328/j.cnki.jos.005771]

© 中国科学院软件研究所 http://www.jos.org.cn

[4] Aitzhan NZ, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. on Dependable and Secure Computing, 2018,15(5):840–852. [doi: 10.1109/TDSC.2016.2616861]

[5] Li L, Liu JQ, Cheng LC, Qiu S, Wang W, Zhang XL, Zhang ZH. CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Trans. on Intelligent Transportation Systems, 2018,19(7):2204–2220. [doi: 10.1109/TITS.2017.2777990]

[6] He YH, Li MR, Li H, Sun LM, Xiao K, Yang C. A blockchain based incentive mechanism for crowdsensing applications. Journal of Computer Research and Development, 2019,56(3):544–554 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2019.20170670]

[7] Yin H, Zhang X, Zhao S. Tradeoffs between cost and performance for CDN provisioning based on coordinate transformation. IEEE Trans. on Multimedia, 2017,19(11):2583–2596. [doi: 10.1109/TMM.2017.2696309]

[8] Liang L, Wu YF, Feng G. Resource allocation algorithm of network slicing based on online auction. Journal of Electronics and Information Technology, 2019,41(5):1187–1193 (in Chinese with English abstract). [doi: 10.11999/JEIT180636]

[9] Hong ZC, Chen WH, Huang HW, Guo S, Zheng ZB. Multi-hop cooperative computation offloading for industrial IoT-edge-cloud computing environments. IEEE Trans. on Parallel and Distributed Systems, 2019,30(12):2759–2774. [doi: 10.1109/TPDS.2019.2926979]

[10] Gao GJ, Xiao MJ, Wu J, Huang LS, Hu C. Truthful incentive mechanism for nondeterministic crowdsensing with vehicles. IEEE Trans. on Mobile Computing, 2018,17(12):2982–2997. [doi: 10.1109/TMC.2018.2829506]

[11] Pu LJ, Chen X, Mao GQ, Xie QY, Xu JD. Chimera: An energy-efficient and deadline-aware hybrid edge computing framework for vehicular crowdsensing applications. IEEE Internet of Things Journal, 2019,6(1):84–99. [doi: 10.1109/JIOT.2018.2872436]

[12] Petrov V, Samuylov A, Begishev V, Moltchnov D, Andreev S, Samouylov KE, Koucheryavy Y. Vehicle-based relay assistance for opportunistic crowdsensing over narrowband IoT (NB-IoT). IEEE Internet of Things Journal, 2018,5(5):3710–3723. [doi: 10.1109/JIOT.2017.2670363]

[13] Wu SK, Chen YJ, Wang Q, Li MH, Wang C, Luo XY. CReam: A smart contract enabled collusion-resistant e-auction. IEEE Trans. on Information Forensics and Security, 2019,14(7):1687–1701. [doi: 10.1109/TIFS.2018.2883275]

[14] Zhang MM, Chen C, Wo TY, Xie T. SafeDrive: Online driving anomaly detection from large-scale vehicle data. IEEE Trans. on Industrial Informatics, 2017,13(4):2087–2096. [doi: 10.1109/TII.2017.2674661]

[15] Liang W, Li KC, Long J, Kui XY. An industrial network intrusion detection algorithm based on multi-characteristic data clustering optimization model. IEEE Trans. on industrial Informatics, 2019, 2063–2071. [doi: 10.1109/TII.2019.2946791]

[16] Cai T, Chen WH, Yang ZT, Zheng ZB. A blockchain-assisted trust access authentication system for solid. IEEE ACCESS, 2020. [doi: 10.1109/ACCESS.2020.2987608]

[17] Kang JW, Xiong ZH, Niyato D, Ye DD, Kim DI, Zhao J. Towards secure blockchain-enabled Internet of vehicles: Optimizing consensus management using reputation and contract theory. arXiv: Cryptography and Security, 2018. [doi: arXiv:1809.08387]

[18] Yu Y, Ding YJ, Zhao YQ, Li YN, Zhao Y, Du XJ, Guizani M. LRCoin: Leakage-resilient cryptocurrency based on bitcoin for data trading in IoT. IEEE Internet of Things Journal, 2019,6(3):4702–4710. [doi: 10.1109/JIOT.2018.2878406]

[19] Yang Z, Yang K, Lei L, Zheng K, Leung VCM. Blockchain-based decentralized trust management in vehicular Networks. IEEE Internet of Things Journal, 2019,6(2):1495–1505. [doi: 10.1109/JIOT.2018.2836144]

[20] Jia DY, Xin JC, Wang ZQ, Guo W, Wang GR. ElasticQM: A query model for storage capacity scalable blockchain system. Ruan Jian Xue Bao/Journal of Software, 2019,30(9):2655−2670 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5774.htm [doi: 10.13328/j.cnki.jos.005774]

[21] Cai T, Chen WH, Yu Y. BCsolid: A Blockchain-based Decentralized Data Storage and Authentication Scheme for Solid. Springer-Verlag, 2019. 676–689. [doi: 10.1007/978-981-15-2777-7_55]

[22] Hu ZY, Tang YJ, Yang ZG, Liu WY. Improved scheme based on S-BAC cross-shard consensus protocol. Application Research of Computers, 2019,8(1):1–6 (in Chinese with English abstract). [doi: 10.19734/j.issn.1001-3695.2019.10.0585]

[23] Pan JF, Huang DC. Blockchain dynamic sharding model based on jump hash and asynchronous consensus group. Computer Science, 2020,47(3):273–280 (in Chinese with English abstract). [doi: 10.11896/jsjkx.190100238]

© 中国科学院软件研究所 http://www.jos.org.cn

[24] Qiu XY, Liu LB, Chen WH, Hong ZC, Zheng ZB. Online deep reinforcement learning for computation offloading in blockchain-empowered mobile edge computing. IEEE Trans. on Vehicular Technology, 2019,68(8):8050–8062. [doi: 10.1109/TVT.2019.2924015]

[25] Chen WH, Zhang Z, Hong ZC, Chen C, Wu JJ, Maharjan S, Zheng ZB, Zhang Y. Cooperative and distributed computation offloading for blockchain-empowered industrial internet of things. IEEE Internet of Things Journal, 2019,6(5):8433–8446. [doi: 10.1109/JIOT.2019.2918296]

[26] Wang XM, Wu WW, Qi DY. Mobility-aware participant recruitment for vehicle-based mobile crowdsensing. IEEE Trans. on Vehicular Technology, 2018,67(5):4415–4426. [doi: 10.1109/TVT.2017.2787750]

[27] Ni JB, Zhang AQ, Lin XD, Shen XS. Security, privacy, and fairness in fog-based vehicular crowd sensing. IEEE Communications Magazine, 2017,55(6):146–152. [doi: 10.1109/MCOM.2017.1600679]

[28] Xiao L, Chen TH, Xie CX, Dai HY, Poor HV. Mobile crowdsensing games in vehicular networks. IEEE Trans. on Vehicular Technology, 2017,67(2):1535–1545. [doi: 10.1109/TVT.2016.2647624]

[29] Kiani A, Ansari N. Toward hierarchical mobile edge computing: An auction-based profit maximization approach. IEEE Internet of Things Journal, 2017,4(6):2082–2091. [doi: 10.1109/JIOT.2017.2750030]

[30] Wang LJ, Liu M, Meng MQH. A hierarchical auction-based mechanism for real-time resource allocation in cloud robotic systems. IEEE Trans. on Cybernetics, 2016,47(2):473–484. [doi: 10.1109/TCYB.2016.2519525]

[31] Jin AL, Song W, Wang P, Niyato D, Ju PJ. Auction mechanisms toward efficient resource sharing for cloudlets in mobile cloud computing. IEEE Trans. on Services Computing, 2016,9(6):895–909. [doi: 10.1109/TSC.2015.2430315]

[32] Wen YT, Shi JY, Zhang Q, Tian XH, Huang ZY, Yu H, Cheng Y, Shen XM. Quality-driven auction-based incentive mechanism for mobile crowd sensing. IEEE Trans. on Vehicular Technology, 2015, 4203–4214. [doi: 10.1109/TVT.2014.2363842]

[33] Dong XQ, Guo B, Shen Y, Duan XL, Shen YC. An efficient and secure decentralizing data sharing model. Chinese Journal of Computers, 2018,41(5):1021–1036 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2018.01021]

[34] Wang RH, Zhang LF, Xu QQ, Zhou H. Byzantine fault tolerance algorithm for consortium blockchain. Application Research of Computer, 2019,37(11):1–6 (in Chinese with English abstract). [doi: 10.19734/j.issn.1001-3695.2019.07.0268]

[35] Xu CH, Wang K, Li P, Guo S, Luo JT, Ye BL, Guo MY. Making big data open in edges: A resource-efficient blockchain-based approach. IEEE Trans. on Parallel and Distributed Systems, 2019,30(4):870–882. [doi: 10.1109/TPDS.2018.2871449]

[36] Li M, Weng J, Yang AJ, *et al*. CrowdBC: A blockchain-based decentralized framework for crowdsourcing. IEEE Trans. on Parallel and Distributed Systems, 2019,30(6):1251–1266. [doi: 10.1109/TPDS.2018.2881735]

[37] He YH, Li H, Cheng XZ, Liu Y, Yang C, Sun LM. A blockchain based truthful incentive mechanism for distributed P2P applications. IEEE Access, 2018, 27324–27335. [doi: 10.1109/ACCESS.2018.2821705]

[38] Kang JW, Yu R, Huang XM, Maharjn S, Zhang Y, Hossain E. Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. IEEE Trans. on Industrial Informatics, 2017,13(6):3154–3164. [doi: 10.1109/TII.2017.2709784]

[39] Vijayakumar P, Obaidat M S, Azees MS, Azees M, Islam SKH, Kumar N. Efficient and secure anonymous authentication with location privacy for IoT-based WBANs. IEEE Trans. on Industrial Informatics, 2020,16(4):2603–2611. [doi: 10.1109/tii.2019.2925071]

[40] Erdem E, Sandikkaya MT. OTPaaS—One time password as a service. IEEE Trans. on Information Forensics and Security, 2019, 14(3):743–756. [doi: 10.1109/TIFS.2018.2866025]

[41] Ausubel LM. An efficient ascending-bid auction for multiple objects. The American Economic Review, 2004,94(5):1452–1475. [doi: 10.1257/0002828043052330]

[42] Danezis G, Meiklejohn S. Centrally banked cryptocurrencies. In: Proc. of the Conf. on Network and Distributed System Security Symposium (NDSS). 2016. 1–14. [doi: 10.14722/ndss.2016.23187]

[43] Al-Bassam M, Sonnino A, Bano S, Hrycyszyn D, Danezis G. Chainspace: A sharded smart contracts platform. In: Proc. of the Conf. on Network and Distributed System Security Symp. (NDSS). 2018. 1–16. [doi: 10.14722/ndss.2018.23244]

[44] Luu L, Narayanan V, Zheng CD, Baweja K, Saxena P. A secure sharding protocol for open blockchains. In: Proc. of the ACM SIGSAC Conf. on Computer and Communications Security. 2016. 17–30. [doi: 10.1145/2976749.2978389]

© 中国科学院软件研究所 http://www.jos.org.cn

[45] Kokoris-Kogias E, Jovanovic P, Gasser L, Gailly N, Syta E, Ford B. Omniledger: A secure, scale-out, decentralized ledger via sharding. In: Proc. of the Symp. on Security and Privacy (SP). IEEE, 2018. 583–598. [doi: 10.1109/SP.2018.000-5]

[46] Zamani M, Movahedi M, Raykova M. Rapidchain: Scaling blockchain via full sharding. In: Proc. of the ACM SIGSAC Conf. on Computer and Communications Security. 2018. 931–948. [doi: 10.1145/3243734.3243853]

[47] Wang JP; Wang H. Monoxide: Scale out blockchains with asynchronous consensus zones. In: Proc. of the Symp. on Networked Systems Design and Implementation (NSDI). 2019. 95–112. [doi: 10.13140/RG.2.2.32017.48489]

附中文参考文献:

[1] 谭海波,周桐,赵赫,赵哲,王卫东,张中贤,盛念祖,李晓风.基于区块链的档案数据保护与共享方法.软件学报,2019,30(9):2620–2635. http://www.jos.org.cn/1000-9825/5770.htm [doi: 10.13328/j.cnki.jos.005770]

[3] 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. http://www.jos.org.cn/1000-9825/5771.htm [doi: 10.13328/j.cnki.jos.005771]

[6] 何云华,李梦茹,李红,孙利民,肖珂,杨超.群智感知应用中基于区块链的激励机制.计算机研究与发展,2019,56(3):544–554.

[8] 梁靓,武彦飞,冯钢.基于在线拍卖的网络切片资源分配算法.电子与信息学报,2019,41(5):1187–1193.

[20] 贾大宇,信俊昌,王之琼,郭薇,王国仁.存储容量可扩展区块链系统的高效查询模型.软件学报,2019,30(9):2655–2670. http://www.jos.org.cn/1000-9825/5774.htm [doi: 10.13328/ j.cnki.jos.005774]

[22] 胡振宇,唐颖杰,杨振国,刘文印.基于 S-BAC 跨分片共识协议的改进方案.计算机应用研究.2019,38(1):1–6.

[25] 潘吉飞,黄德才.基于跳跃 Hash 和异步共识组的区块链动态分片模型.计算机科学,2020,47(3):273–280.

[33] 董祥千,郭兵,沈艳,段旭良,申云成,张洪.一种高效安全的去中心化数据共享模型.计算机学报,2018,41(5):1021–1036.

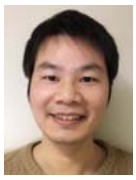
[34] 王日宏,张立锋,徐泉清,周航.可应用于联盟链的拜占庭容错共识算法.计算机应用研究,2019,37(11):1–6.

蔡婷(1984－),女,博士,副教授,主要研究领域为区块链,物联网安全,访问控制,边缘/云计算.

郑子彬(1982－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为区块链,服务计算,软件工程.

林晖(1996－),女,硕士,主要研究领域为博弈论,边缘计算的资源分配和区块链.

余阳(1966－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为工作流,服务计算,云计算,软件工程.



陈武辉(1984－),男,博士,副教授,CCF 专业会员,主要研究领域为边缘/云计算,云机器人,区块链.

© 中国科学院软件研究所 http://www.jos.org.cn