Journal of Computer Applications
计算机应用,2019,39(2):458-463
ISSN 1001-9081
CODEN JYIIDU
2019-02-10
http://www.joca.cn

文章编号:1001-9081(2019)02-0458-06
DOI:10.11772/j.issn.1001-9081.2018061247

基于区块链技术的物联网信息共享安全机制

葛　琳[1,2*],季新生[3],江　涛[3],江逸茗[3]

(1.郑州航空工业管理学院 计算机学院,郑州 450046;　2.中国民航大学 中国民航信息技术科研基地,天津 300300;
3.国家数字交换系统工程技术研究中心,郑州 450002)

(*通信作者电子邮箱 lingesnow@126.com)

摘　要:针对物联网(IoT)信息共享中存在的源数据易被篡改、缺乏信用保障机制以及信息孤岛问题,提出一种基于区块链技术的轻量级物联网信息共享安全框架。该框架采用数据区块链和交易区块链相结合的双链模式:在数据区块链中实现数据的分布式存储和防篡改,并通过改进的实用拜占庭容错(PBFT)机制共识算法,提升数据登记效率;在交易区块链中实现资源和数据交易,并通过基于部分盲签名算法的改进算法,提升交易效率、实现隐私保护。仿真实验部分分别针对抗攻击能力、双链的处理能力和时延进行了验证分析,结果表明该框架具有安全性、有效性和可行性,可应对现实物联网中的大部分场景。

关键词:物联网;区块链;信息共享安全;共识算法;去中心化

中图分类号:TP309　　**文献标志码**:A

Security mechanism for Internet of things information sharing based on blockchain technology

GE Lin[1,2*], JI Xinsheng[3], JIANG Tao[3], JIANG Yiming[3]

(1. *College of Computer, Zhengzhou University of Aeronautics, Zhengzhou Henan* 450046, *China*;
2. *Information Technology Research Base of Civil Aviation Administration of China, Civil Aviation University of China, Tianjin* 300300, *China*;
3. *National Digital Switching System Engineering and Technological R&D Center, Zhengzhou Henan* 450002, *China*)

Abstract: A lightweight framework of Internet of Things (IoT) information sharing security based on blockchain technology was proposed to solve the problems of IoT's information sharing, such as source data susceptible to tampering, lack of credit guarantee mechanism and islands of information. The framework used double-chain pattern including data blockchain and transaction blockchain. Distributed storage and tamper-proof were realized on the data blockchain, and the registration efficiency was improved through a modified Practical Byzantine Fault Tolerance (PBFT). Resource and data transactions were realized on the transaction blockchain, the transaction efficiency was improved and privacy protection was realized through the improved algorithm based on partial blind signature algorithm. The simulation experiments were carried out to analyse, test and verify anti-attack capability, double-chain processing capacity and time delay. Simulation results show that the proposed framework has security, effectiveness and feasibility, which can be applied to most situations of the real IoT.

Key words: Internet of Things (IoT); blockchain; information sharing security; consensus algorithm; decentralization

0　引言

自2005年国际电信联盟正式提出物联网(Internet of Things, IoT)概念以来,物联网产业发展迅猛,目前被广泛地应用于环境监测与保护、智能交通、移动医疗、食品安全和物流供应链管理等诸多领域[1]。根据Statistic门户网站最新统计数据,2017年物联网的互联设备数量约为203.5亿,预计到2020年将增长至307.3亿[2],市场规模将达7.1万亿美元[3]。物联网信息具有多源异构、规模巨大、时空关联、冗余度高、多维标量等特征[4],经过大数据整合,可以产生全新的生产、生活和服务维度。物联网不同应用场景之间的信息共享,可实现对现实世界各类物体的信息采样、智能追踪、监控和管理[5],从而改造人类社会,真正走向智慧家居、智慧城市、智慧地球,具有重要的理论意义和社会经济价值。

目前,由于担心数据被非法篡改或因交互而导致数据丢失等原因,物联网中缺乏有效的共享机制,从而难以实现数据有价值的互联互通。物联网信息共享的安全问题已成为信息安全领域中的热点和难点[1,6]。物联网现有系统间信息的交互和交易,要么选择线下进行,要么采用基于云服务的信息共享技术。这些机制存在诸多不足:1)大多只考虑信息传输中的某一环节,或仅针对某一应用场景、逻辑层次、安全属性等单一角度,适用范围较窄;2)面对庞大的物联网络和由此产生的海量数据,中心化数据处理的基础设施投入和维护成本高,效率低,且难以应对数据的指数倍增长;3)缺乏有效的网络信用保障机制,以确保物联网设备的合法身份、信息有效性,信息在不同系统传递过程中的真实性、一致性和不可被篡

收稿日期:2018-06-15;**修回日期**:2018-09-16;**录用日期**:2018-09-17。

基金项目:中国民航信息技术科研基地开放课题基金资助项目(CAAC-ITRB-201707);国家自然科学基金创新研究群体项目(61521003);国家重点研发计划项目(2017YFB0801903);国家自然科学基金资助项目(61502530)。

作者简介:葛琳(1978—),女,山东济南人,博士,讲师,CCF会员,主要研究方向:网络信息安全;　季新生(1969—),男,江苏南通人,教授,博士生导师,博士,主要研究方向:网络安全;　江涛(1974—),男,湖北武汉人,副研究员,硕士,主要研究方向:移动互联网安全;　江逸茗(1984—),男,江苏南通人,博士,主要研究方向:网络信息安全。

改性;4)物联网中的射频识别装置、红外感应器等信息传感设备节点的运算、传输等资源都受限,在对信息进行保护时还需兼顾数据的可用性和效率[5-9]。

近年来,区块链技术的研究与应用呈现爆发式增长态势,被认为是继大型机、个人电脑、互联网、移动/社交网络之后计算范式的第五次颠覆式创新[10]。在 Gartner 技术成熟度曲线中,区块链技术处于高期望值区,在未来发展趋势的数字平台领域,也位列其中[11];2016 年,工信部发布了《中国区块链技术和应用发展白皮书》[12];在国务院发布的《"十三五"国家信息化规划》中[13],明确指出要加强区块链等新技术的基础研发和前沿布局,正式从国家科技战略层面肯定了区块链的技术与社会价值。区块链技术具有高度透明、去中心化、去信任、集体维护等性质,能够通过运用数据加密、时间戳、分布式共识和智能合约等手段,在节点无需互相信任的物联网分布式系统中,实现基于去中心化信用的交互方式,为解决中心化架构普遍存在的高成本、低效率等问题提供了解决途径。物联网信息摘要可保存在区块链中,形成可信的物联网数据来源,区块链特有的数据加密和验证机制能够有效保护数据安全,并维护数据方隐私,攻击者即使侵入网络,也无法窃取真实数据内容,更无法对数据进行篡改。区块链技术使得物联网智能节点间的资源交易成为可能,对未来信息互联网向价值互联网的转变具有重要的现实意义[14-16]。

区块链技术的快速发展引起了政府部门、金融机构、科技企业和资本市场的广泛关注。在金融领域,各国中央银行高度重视区块链技术,通过借鉴研究或直接应用区块链来设计各自的法定数字货币。同时,区块链技术的潜力吸引了众多知名企业和政府部门致力于此项研究,如:IBM 与三星的合作项目"去中心化的点对点自主遥测(Autonomous Decentralized Peer-to-Peer Telemetry, Adept)"[17];工业和信息化部中国电子技术标准化研究院先后发布了《区块链 参考架构》和《区块链 数据格式规范》标准[18-19],旨在利用区块链为物联网开发分布式平台。在科研学术领域,国外将区块链技术应用于物联网的研究呈现逐年上升趋势,如:文献[20-21]强调了通过区块链技术保障用户拥有物联网数据的优点,拥有私人信息的用户可以选择将数据出售给第三方;文献[22]中描述了一种基于区块链技术的可审计的物联网数据存储和共享机制;在文献[23]中,利用区块链开发平台 Ethereum 的可编程性,以细粒度的方式提供物联网设备管理;文献[24]提出了一种针对物联网区块链的分层体系结构。我国国内针对此类的研究也已起步,主要针对某一具体应用场景[25-26]。综上所述,将区块链技术应用于物联网中,已有理论基础论述和实际项目研发;然而,如何利用区块链技术解决物联网中的信息安全问题仍处于探索阶段,基于区块链技术的物联网信息共享安全机制尚未有系统性的研究。

本文的主要工作为:利用区块链的特征,尝试性地将区块链技术应用于物联网,设计了基于区块链的轻量级物联网信息共享安全机制;采用数据区块链和交易区块链相结合的双链方式,实现物联网的数据源安全和信息交互安全,并为当前普遍存在的数据孤岛问题提供了解决思路。仿真实验结果表明,该方案具有安全性、有效性和可行性。

1　基于区块链技术的物联网信息共享

1.1　理论分析

物联网信息共享安全的目的是:在确保信息安全的前提下实现共享。信息安全包括了信息的保密性、完整性和可用性,也含有其他特性,如真实性、可追溯、抗抵赖和可靠性[8]。

区块链技术借助分布式系统各节点的工作量证明(Proof of Work, PoW)等共识算法形成的强大算力来抵御外部攻击,保证区块数据的不可篡改和不可伪造,通过对双重支付问题和拜占庭将军问题的解决,在无需信任单个节点的情况下构建一个去中心化的可信任系统,在信息传输的过程中同时完成价值的转移,满足了对可用性和可靠性的需求。

为满足安全性和所有权验证,将诸如 RSA(Rivest-Shamir-Adleman)、Elgamal、Rabin、D-H(Diffie-Hellman)、椭圆曲线加密(Elliptic Curves Cryptography, ECC)等算法集成到区块链中,形成非对称加密和多重签名机制,满足了对保密性的需求。

区块链系统常用的 Merkle 树及其变种,支持简化支付验证(Simplified Payment Verification, SPV),可在不必存储完整区块链的情况下,对交易进行验证,满足了对完整性的需求。此外,Merkle 树对区块链运行效率的提升和仅需保存部分区块数据的特点,也使得将区块链技术运用在物联网设备上成为可能。

区块链系统使用密码学技术对数据进行保护,数据在写入区块前需经过全体节点验证,写入后区块链网络各节点可公开查询,有助于消除信息优势、降低信任成本,满足了对真实性的需求。

区块链中获得记账权的节点必须在当前区块头中加盖时间戳,作为区块数据的写入时间。因此,主链上各区块是按照时间顺序依次排列的。时间戳作为区块数据的存在性证明(Proof of Existence, PoE),为数据增加了时间维度,具有极强的可验证性,结合区块链的链式结构,满足了对可追溯的需求。

区块链中新生成的数据必须获得全部或大多数节点的验证通过后,才可写入共享账本,而该账本由全体区块链节点共同维护,因而极难篡改和伪造,满足了对抗抵赖的需求。

1.2　基于区块链技术的物联网信息共享安全框架

本文提出了一种基于区块链技术的物联网信息共享安全框架,其中包括源数据采集和信息交易,对应源数据安全和交互安全形成信息共享安全体系,如图 1 所示。根据物联网的分层理念,分为感知层、传输层和应用层。框架采用数据区块链和交易区块链双链模式。由于物联网部分节点的资源有限,因此将双链的部分功能实现外包给云服务/雾计算进行,其中,雾计算靠近物联网终端节点,即数据区块链部分;云服务则主要针对应用层的交易区块链,如图 2 所示。对于数据区块链和交易区块链的组成和共识算法设计将在本文的第 2 章进行介绍。

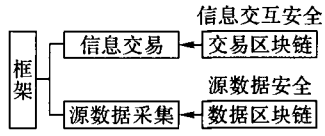

图 1　信息共享安全

Fig. 1　Information sharing security

传统的区块链应用大多基于公有链,任意节点可以自由加入区块链网络并维护账本数据,使得公有链虽然具有较高的公信力,但身份和数据隐私受到威胁。据此,本文采用私有链、联盟链和公有链相结合的方式,如图 3 所示。首先,物联网不同的场景间采用公有链;其次,场景内不同区域间采用联盟链,同一行业的不同部门之间构成联盟,只有联盟成员可维护区块链数据,其他非授权节点则不能;最后,区域内的节点间采用私有链,只有内部节点才能维护区块链数据,从根本上

杜绝了非授权节点接触区块链数据的可能。由于数据区块链主要针对源数据采集,时效性和安全性需求较交易区块链更高,因此采用私有链方式;交易区块链则可根据具体应用场景采用联盟链或者公有链方式。

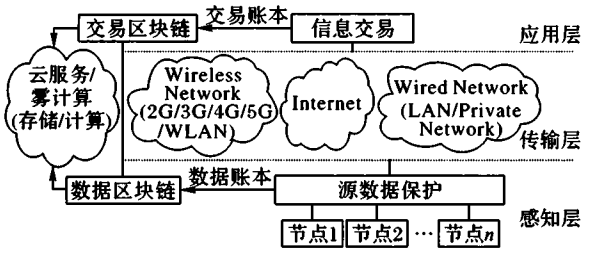

图 2 基于区块链的物联网信息共享安全框架

Fig. 2 Architecture of IoT information sharing security based on blockchain

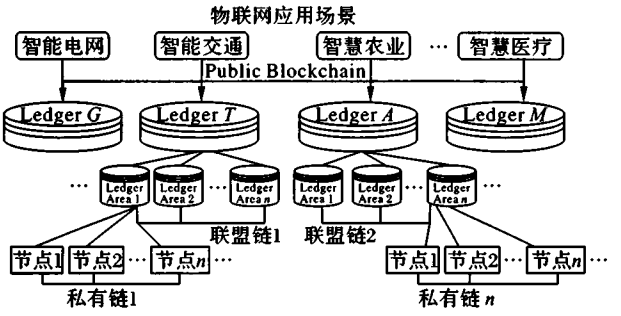

图 3 私有链、联盟链和公有链的框架结构

Fig. 3 Architecture of private blockchain, consortium blockchain and public blockchain

2 基于区块链技术的双链模式

2.1 数据区块链

为避免人为篡改或破坏物联网前端采集设备的传感数据,特别是中心化网络中拥有系统管理权限的人员可能参与伪造/增加/删改数据,确保源数据可靠可信是实现整个信息共享的基础。数据区块链通过物联网节点进行数据采集,利用共识机制形成数据账本。

2.1.1 数据预处理机制

物联网中如射频识别装置、红外感应器等信息传感设备这类节点的运算、存储和传输等资源受到极大的限制;另外,即使如可穿戴等智能设备节点具备一定的能力,轻量级数据的计算和存储也应减少冗余、提高效率。因此,针对物联网中的海量异构数据需进行分类、统一数据表达式和分布存储等操作。首先,将物联网数据分为轻量级数据和多媒体数据,对多媒体数据进行压缩和融合,减少数据容量,提高数据质量。然后,通过统一数据表达式使得数据存储规范、易于共享。最后,将处理后的数据分为账本数据和外包存储数据进行分布存储,其中账本数据为数据摘要,存储于节点,外包数据为大规格或多媒体数据,存储于雾节点,需要时可即时下载。具体如图 4 所示。

2.1.2 拜占庭容错机制共识算法的改进

目前,区块链中常用的共识算法,是为了解决分布式系统中的一致性问题而提出的,然而,这些算法计算时间长、耗费资源大,不适合轻量级、重效率的物联网。因此,本文对实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)算法进行了改进。在改进算法中,只要参与共识计算的错误节点数量不超过 $f=(n-1)/3$ [27],就能保证整个体系的正常运行。其中,n 表示参与共识的节点数量。在改进算法中,每轮共识的数据集合序号记为 s,从 0 开始,每轮共识指定一个议长节点,其序号为 $p=(h_b-s) \bmod n$(其中,h_b 为区块高度)。如果此次共识无法达成,则集合 s 递增,直至共识达成。共识时间间隔为 t,一旦产生新的区块则新一轮共识开启,并置集合序号 $s=0$。共识算法的主要流程如图 5 所示。数据区块链对于数据账本的处理时间和延迟实验将在本文的第 3 章进行。

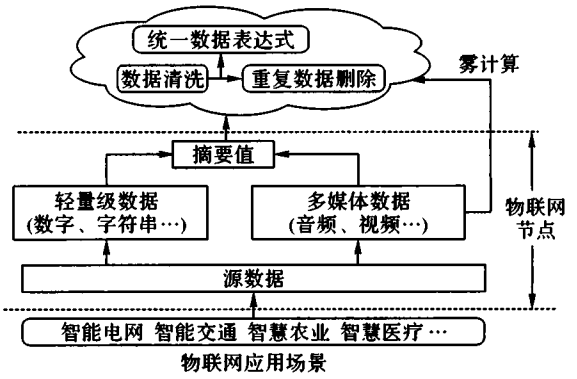

图 4 数据预处理

Fig. 4 Data pre-processing

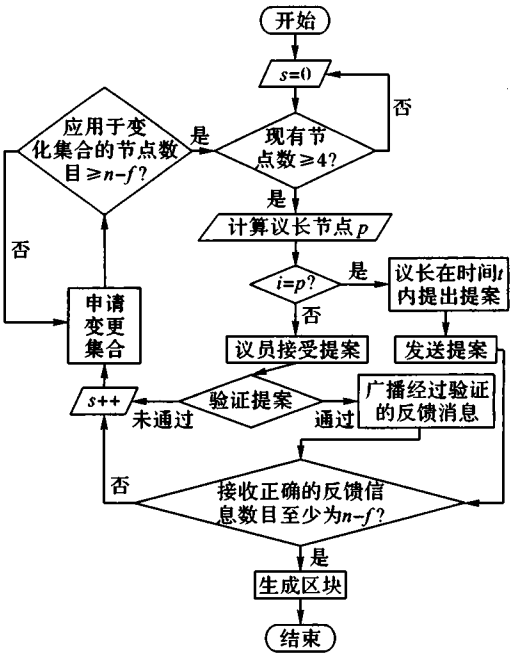

图 5 共识算法流程

Fig. 5 Flow of consensus algorithm

2.2 交易区块链

交易区块链主要为物联网不同节点间的交易支付活动、行为记录等提供去中心、防篡改、可追溯的高效账单生成和可信记账支撑。

2.2.1 分布式记账系统

系统可考虑采取两种记账方式:一是引入代币或者具有法币效力的各类数字货币,作为价值交换的媒介;二是通过算力和信誉等多维度信息的竞争换取记账权,这种方法有利于智能节点的自我发展,即"能者多劳"。两种记账方式的交易记录均需向全网广播,从而确保每一个参与的节点均有机会存储账单副本。物联网节点既可作为云服务的消费者(Cloud Service Consumer, CSC),也可作为云服务的提供者(Cloud Service Provider, CSP)。

2.2.2 部分盲签名算法的改进

为了避免多重支付问题,比特币应用的区块链技术中,一个区块的生成大约需要 10 min,且要等待至少 6 个区块才能

确认付款有效,带来了交易时间过长的问题;与此同时,使用公共总账来记录交易信息也带来了潜在的隐私泄露问题。虽然攻击者无法从公钥账户获取用户真实身份,但可以通过追踪 IP 地址,以及分析区块链上交易的拓扑结构来发现用户的隐私。为解决上述问题,本文提出了一种基于部分盲签名算法的改进算法,利用云服务设立具有可信公钥地址的混币中心(MixCenter, MC),作为实际支付方,缩短交易确认时间,同时使用部分盲签名算法和一次性公钥地址,更好地保护用户隐私[28]。相关符号说明如表 1 所示。交易区块链中交易账本的处理时长和时延测试将在本文的第 3 章进行。

表 1　符号说明

Tab. 1　Symbol description

符号标识	具体含义
w	预存交易金的货币数量
t_e	预存交易金时向 MC 支付的截止时间
p_{adv}	预存交易金时的公钥地址
p_{tmp}	每次交易的一次性公钥地址
σ_C	MC 生成的接受预存承诺
σ_{MC}	MC 生成的预存交易金到账签名
σ_{Vender}	CSP 生成的交易承诺
σ^*_{CSC}	盲化的支付信息
σ_{Pay}	含有盲因子的支付承诺
σ^*_{Pay}	支付承诺
$\sigma_{receive}$	CSC 生成的收货凭证

算法的具体过程大致可描述如下:

1)系统建立。

建立系统参数,MC 生成公私钥对。

2)交易准备。

①CSC 发送 (w, t_e, p_{adv}) 给 MC,申请预存数量 w 的交易金;

②若 MC 受理,生成 σ_C 发送给 CSC;

③CSC 在截止时间 t_e 前将公钥地址 p_{adv} 的货币 w 支付给 MC;

④MC 收到货币 w 后,生成签名 σ_{MC} 并发送给 CSC,完成预存。

3)交易申请。

①CSC 为本次交易生成一次性公钥地址 p_{tmp},作为向 CSP 的付款地址,并连同其他交易相关参数一起发送给 CSP,申请进行数据共享交易;

②CSP 收到申请后,若确认交易,则计算获取公钥地址 p_{tmp},生成签名 σ_{Vender} 作为交易承诺发送给 CSC。

4)交易签名。

①CSC 获得交易承诺后,向 MC 发送 σ_{MC} 及盲化后的含有付款地址 p_{tmp} 的支付信息 σ^*_{CSC};

②MC 签名 σ_{MC},若合法,则调用部分盲签名算法,生成嵌入有共识信息的盲签名 σ^*_{Pay},发送给 CSC。

5)交易付款。

①CSC 将 σ^*_{Pay} 去盲,得到含有付款地址的支付承诺 σ_{Pay},匿名发送给 MC;

②MC 验证 σ_{Pay},若合法,则向一次性公钥地址 p_{tmp} 支付 w 数量的货币。

6)交易成功。

①CSP 监测到区块链上 MC 向一次性公钥地址 p_{tmp} 付款,执行交易承诺,向 CSC 开放数据访问权限或将数据发送给 CSC;

②CSC 获取数据后,生成签名 $\sigma_{receive}$ 作为交付凭证发送给 CSP,交易结束。

3　实验结果与分析

本章将通过仿真实验对本文提出的框架可能受到的安全威胁及采取的应对机制进行分析,并给出抵抗能力评估;同时对数据区块链和交易区块链的性能进行仿真测试。

3.1　抗攻击能力

本节对基于区块链技术的物联网信息共享安全框架的安全性进行分析。在表 2 中,涵盖了 10 个物联网/区块链易受的特定攻击,结合本文的机制方案给出防范方法,并基于欧洲电信标准协会(European Telecommunications Standards Institute, ETSI)风险分析标准,定义了本框架可抵御各种攻击的能力。从表 2 中可以看出,本框架对 6 种攻击有超高抵抗力,对 3 种攻击有高抵抗力,对 1 种具有中等/高抵抗力。分析原因为,如果攻击节点遵照流程进行入网注册、分配公私钥等操作,在这种情况下是无法将其与正常节点进行区别的,除非该节点有进一步的攻击行为,而通过私有链的节点将大幅降低此类风险。本文图 2 的框架结构中,物联网节点可按照地域归属不同的私有链(Private Blockchain, PrBC)。

3.2　数据区块链性能

本节对数据区块链的数据账本吞吐量和时延进行测试,以验证其有效性和可行性。数据区块链仿真系统实验设计分为数据产生模块和共识模块。数据产生模块负责数据生成模拟,向共识模块发送请求,以测试共识模块的账本确定时间和系统的每秒交易数(Transactions Per Second, TPS)。仿真系统采用 Java 语言编写,在单机环境模拟 1 个数据产生进程,9 个共识执行进程。系统运行环境:Intel Core m7-6Y75 1.51 GHz 的 CPU, 8 GB 内存,CentOS 7 操作系统,JDK 版本为 1.8.0。仿真实验时,数据产生模块持续向共识模块发送请求,共识模块执行改进的 PBFT 算法,达成共识后,将数据写入新的区块,记入全网账本。

1)吞吐量。数据区块链中交易吞吐量(TPS)指节点采集数据上传,发送数据摘要请求到共识确认写入账本的总交易数除以时间。分别取 10 s,20 s,40 s,60 s,100 s 等不同的区块产生时间,每时间段重复测试 10 次,取 10 次平均值作为该时间段的 TPS,测试结果如图 6 所示。由图可知,数据区块链的交易吞吐量约为 9 500 次/s,可以应对现实物联网中的大部分场景。

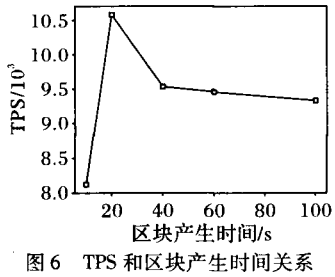

图 6　TPS 和区块产生时间关系

Fig. 6　Relationship of TPS and block generation time

2)时延。数据区块链的时延为请求发生到账本确认的时间间隔,由请求广播传输时间、共识算法执行时间和广播确认时间组成。按前文的 5 个区块产生时间,统计所有时延的平均值,得到不同区块产生时间下账本时延的关系如图 7 所示。可以看出,区块产生时间越长,时延也越长。分析原因为,随着区块产生的时间增加,在时间段内收到的请求会更多,广播和验证的时间更长,广播确认的区块更大,造成总的时延增加。对比吞吐量关系图,TPS 最大时的区块产生时间

对应的时延是ms级,可被大多数物联网应用场景所接受。

3.3 交易区块链性能

交易区块链交易过程中的主要时间消耗为创建交易、签名计算和确认收货的时间。其中,创建交易的时间指初始化、消息发起和确认时间的累计,与物联网的网络通信状况等相关;确认收货时间则与参与监管的智能合约复杂程度等相关。本节仅针对签名计算时间进行分析。本文选用可高效实现的短签名算法,优化签名计算的时间消耗,提高账本的处理效率。仿真实验选用门限签名(THreshold Signature, THS)短签名算法,签名长度160 bit,进行500次仿真,时间消耗平均值为:参数生成64.26 ms,签名20.02 ms,验证26.52 ms,合计110.80 ms。与需要约1 h确认时间的比特币系统相比,本机制下的交易区块链账本生成效率更高。

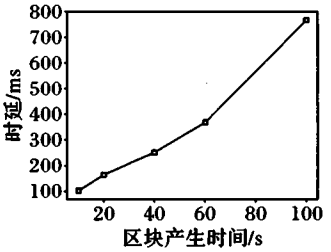

图7 账本时延和区块产生时间关系

Fig. 7 Relationship of ledger delay and block generation time

表2 物联网/区块链攻击分析及应对机制

Tab. 2 IoT/Blockchain attack analysis and response mechanism

序号	攻击类别	攻击方式	防御机制
1	追加攻击	攻击者通过伪造交易和创造虚假共识生成区块	物联网节点可以通过验证账本的输出和所有者,在验证步骤检测出虚假区块
2	拒绝服务攻击(DoS)	攻击者向目标节点发送超出其处理能力的大量交易,使其没有资源处理来自其他节点的真实交易	1)物联网节点不会向其他节点发送交易,除非与其密钥列表中的实体匹配; 2)每个PrBC间的交叠节点具有交易的最大速率的阈值。如果超过阈值,则更新密钥列表以防止节点向目标节点持续发送交易
3	分布式拒绝服务攻击(DDoS)	攻击者利用多个节点进行拒绝服务攻击	1)由于使用非对称加密的密钥管理机制,所以感染设备节点是非常困难的; 2)在PrBC中,只有在节点之间建立共享密钥,节点设备才能与其他设备通信; 3)不同PrBC节点之间在进行信息交互之前需得到授权; 4)使用双链结构,在数据区块链中,信息交易是无效的,反之亦然; 5)防止DoS攻击的方法对于防治DDoS也是有用的
4	设备注入攻击	攻击者将虚假节点注入网络,以获取访问隐私信息的能力	注入的设备会被隔离,因为本地通信要求PrBC节点间已经建立了共享密钥
5	链接攻击	攻击者将云中的多个数据或区块链中的交易用相同的ID链接起来,以找到匿名节点对应的真实世界标识	节点在交易中使用唯一的私钥,并使用部分盲签名算法和一次性公钥地址
6	丢弃攻击	争取到记账权的节点丢弃其成员的交易,从而将其隔离	当节点发现它的交易一直没有被处理时,可以改变其关联的PrBC,向邻近PrBC发起请求
7	修改攻击	恶意云存储修改或移除存储的数据	存储交易中包括已存储数据的哈希值,用作已存储数据或上次修改时间的证据,以发现数据是否被修改或移除,但是,一旦修改将无法恢复
8	公共区块修改	攻击者广播一个区块的虚假账本,并将其作为最长账本,导致其他节点将攻击者的账本作为真实账本	使用的共识算法限制了一个时间间隔内可以产生的区块数量,这也就限制了可以增加的恶意区块的数量,因此防止了攻击者产生最长账本,并将其作为真实账本
9	破坏时间间隔	恶意记账节点在一个共识周期产生多个区块	节点可以检测到它们在一个共识周期内收到了超过允许数量的区块,这会降低恶意节点的信任率,直至其被隔离
10	共识周期攻击	攻击者发送虚假请求更新共识周期	请求生效需要至少超过一半节点的签名,可能性非常低

4 结语

针对物联网信息共享缺乏信用保障机制以及信息孤岛问题,开展了数据防篡改、去中心化等方面的研究,本文提出了一种轻量级信息共享安全机制:1)基于区块链技术,采用数据区块链和交易区块链双链模式,实现对源数据采集和信息交易的保护;2)数据区块链利用共识机制形成数据账本,防止人为篡改或破坏采集数据;3)交易区块链使用分布式记账系统,实现账单的防篡改和可追溯。

本文主要采用区块链技术解决物联网信息共享安全问题,然而,在具体行业应用时,其性能还有待增强,隐私泄露风险也亟待解决。下一步,将重点研究区块链的数据的高并发处理和隐私保护问题,进一步提高本文提出框架的实用性。

参考文献:

[1] 张玉清,周威,彭安妮.物联网安全综述[J].计算机研究与发展,2017,54(10):2130-2143.(ZHANG Y Q, ZHOU W, PENG A N. Survey of things security [J]. Journal of Computer Research and Development, 2017, 54(10): 2130-2143.)

[2] Statista Inc. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions) [EB/OL]. [2017-05-30]. http://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide.

[3] Ironpaper. Internet of things market statistics — 2016 [EB/OL]. [2017-04-08]. http://www.ironpaper.com/webintel/articles/internet-of-things-market-statistics/.

[4] LI T, LIU Y, TIAN Y, et al. A storage solution for massive IoT data based on NoSQL [C]// Proceedings of the 2012 IEEE International Conference on Internet of Things. Washington, DC: IEEE Computer Society, 2012: 50-57.

[5] 田野,袁博,李廷力.物联网海量异构数据存储与共享策略研究[J].电子学报,2016,44(2):247-257.(TIAN Y, YUAN B, LI T L. A massive and heterogeneous data storage and sharing strategy for

internet of things [J]. Acta Electronica Sinica, 2016, 44(2): 247 - 257.)

[6] 董晓蕾. 物联网隐私保护研究进展[J]. 计算机研究与发展, 2015, 52(10): 2341 - 2352. (DONG X L. Advances of privacy preservation in Internet of things [J]. Journal of Computer Research and Development, 2015, 52(10): 2341 - 2352.)

[7] 姜顺荣. 物联网中信息共享的安全和隐私保护的研究[D]. 西安: 西安电子科技大学, 2016: 55 - 65. (JIANG S R. Research on secure and privacy-preserving of information sharing in Internet of things [D]. Xi'an: Xidian University, 2016: 55 - 65.)

[8] 桂小林, 张学军, 赵建强, 等. 物联网信息安全[M]. 北京: 机械工业出版社, 2015. (GUI X L, ZHANG X J, ZHAO J Q, et al. Information Security of IoT [M]. Beijing: China Machine Press, 2015.)

[9] 史佩昌, 王怀民, 郑子彬, 等. 面向云际计算的自主对等协作环境[J]. 中国科学: 信息科学, 2017, 47(9): 1129 - 1148. (SHI P C, WANG H M, ZHENG Z B, et al. Collaboration environment for joint cloud computing [J]. Scientia Sinica Informationis, 2017, 47(9): 1129 - 1148.)

[10] SWAN M. Blockchain: Blueprint for a New Economy [M]. Sebastopol, CA: O'Reilly Media Inc., 2015: 13 - 14.

[11] PANETTA K. Top Trends in the gartner hype cycle for emerging technologies [EB/OL]. [2017-08-15]. https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies - 2017/.

[12] 中国区块链技术和产业发展论坛. 中国区块链技术和应用发展白皮书(2016) [EB/OL]. [2017-11-18]. http://chainb.com/download/工信部 - 中国区块链技术和应用发展白皮书 1014.pdf. (China Blockchain Technology and Industrial Development Forum. China blockchain technology and application development white paper (2016) [EB/OL]. [2017-11-18]. http://chainb.com/download/工信部 - 中国区块链技术和应用发展白皮书 1014.pdf.)

[13] 国务院. 国务院关于印发"十三五"国家信息化规划的通知[EB/OL]. [2016-12-27]. http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm. (State Council. Notice of the state council on printing and distributing the "13th Five-Year" national informatization plan [EB/OL]. [2016-12-27]. http://www.gov.cn/zhengce/content/2016 - 12/27/content _ 5153411.htm.)

[14] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2018-03-21]. https://bitcoin.org/bitcoin.pdf.

[15] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481 - 494. (YUAN Y, WANG F Y. Blockchain: the state of the art and future trends [J]. Acta Automatica Sinica, 2016, 42(4): 481 - 494.)

[16] 王继业, 高灵超, 董爱强, 等. 基于区块链的数据安全共享网络体系研究[J]. 计算机研究与发展, 2017, 54(4): 742 - 749. (WANG J Y, GAO L C, DONG A Q, et al. Block chain based data sharing network architecture research [J]. Journal of Computer Research and Development, 2017, 54(4): 742 - 749.)

[17] IBM. ADEPT: an IoT practitioner perspective[EB/OL]. [2017-05-07]. https://zh.scribd.com/doc/252917347/IBM-ADEPT-Practictioner-Perspective-Pre-Publication-Draft-7-Jan-2015.

[18] 中国电子技术标准化研究院. 区块链 参考架构[EB/OL]. [2017-05-17]. http://www.cesi.ac.cn/201705/2478.html. (China Electronics Standardization Institute. Blockchain — Reference Architecture[EB/OL]. [2017-12-27]. http://www.cesi.ac.cn/201705/2478.html.)

[19] 中国电子技术标准化研究院. 区块链 数据格式规范[EB/OL]. [2017-12-27]. http://www.cesi.ac.cn/images/editor/20171227/20171227154118126.pdf. (China Electronics Standardization Institute. Blockchain - Data format specification [EB/OL]. [2017-12-27]. http://www.cesi.ac.cn/images/editor/20171227/20171227154118126.pdf.)

[20] ZHANG Y, WEN J. An IoT electric business model based on the protocol of bitcoin [C]// Proceedings of the 2015 International Conference on Intelligence in Next Generation Networks. Piscataway, NJ: IEEE, 2015: 184 - 191

[21] WÖRNER D, von BOMHARD T. When your sensor earns money: exchanging data for cash with bitcoin [C]// Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication. New York: ACM: 295-298.

[22] HOSSEIN S, HITHNAWI A, DUQUENNOY S. Towards blockchainbased auditable storage and sharing of IoT data [EB/OL]. [2018-03-05]. https://arxiv.org/pdf/1705.08230.pdf.

[23] OUADDAH A, ELKALAM A A, OUAHMAN A A. Towards a novel privacy-preserving access control model based on blockchain technology in IoT [C]// Proceedings of the 2017 Europe and MENA Cooperation Advances in Information and Communication Technologies, AISC 520. Cham: Springer, 2017: 523 - 533.

[24] DORRI A, KANHERE S S, JURDAK R. Towards an optimized blockchain for IoT [C]// Proceedings of the 2017 Second International Conference on IoT Design and Implementation. New York: ACM, 2017: 173 - 178

[25] 张俊, 高文忠, 张应晨, 等. 运行于区块链上的智能分布式电力能源系统: 需求、概念、方法以及展望[J]. 自动化学报, 2017, 43(9): 1544 - 1554. (ZHANG J, GAO W Z, ZHANG Y C, et al. Blockchain based intelligent distributed electrical energy systems: needs, concepts, approaches and vision [J]. Acta Automatica Sinica, 2017, 43(9): 1544 - 1554.)

[26] 薛腾飞, 付群超, 王枞, 等. 基于区块链的医疗数据共享模型研究[J]. 自动化学报, 2017, 43(9): 1555 - 1562. (XUE T F, FU Q C, WANG C, et al. A medial data sharing model via blockchain [J]. Acta Automatica Sinica, 2017, 43(9): 1555 - 1562.)

[27] 黄晓芳, 徐蕾, 杨茜. 一种区块链的云计算电子取证模型[J]. 北京邮电大学学报, 2017, 40(6): 120 - 124. (HUANG X F, XU L, YANG Q. Blockchain model of cloud forensics[J]. Journal of Beijing University of Posts and Telecommunications, 2017, 40(6): 120 - 124).

[28] 傅晓彤, 陈思, 张宁. 基于代理的密码货币支付系统[J]. 通信学报, 2017, 38(7): 199 - 206. (FU X T, CHEN S, ZHANG N. Proxy-cryptocurrency payment system [J]. Journal on Communications, 2017, 38(7): 199 - 206).

This work is partially supported by the Open Project Foundation of Information Technology Research Base of Civil Aviation Administration of China (CAAC-ITRB-201707), the Innovative Research Groups of National Natural Science Foundation of China (61521003), the National Key Research and Development Program of China (2017YFB0801903), the National Natural Science Foundation of China (61502530).

GE Lin, born in 1978, Ph. D., lecturer. Her research interests include network information security.

JI Xinsheng, born in 1969, Ph. D., professor. His research interests include network security.

JIANG Tao, born in 1974, M. S., associate research fellow. His research interests include mobile Internet security.

JIANG Yiming, born in 1984, Ph. D. His research interests include network information security.