2019 年 11 月 第 11 期
Vol. 40 No. 11 2019

基于区块链的物联网数据共享模型

于金刚[1,2],张 弘[1,2],李 姝[3],毛立爽[2],姬鹏翔[2]

[1](中国科学院大学,北京 100049)
[2](中国科学院 沈阳计算技术研究所,沈阳 110168)
[3](沈阳理工大学,沈阳 110159)
E-mail: zhanghong16@mails.ucas.ac.cn

摘 要: 随着物联网技术的进步,物联网结构变得日益复杂,采集的数据量呈现爆发式增长,如何在不同的参与方间安全地共享数据成为了一个巨大的挑战. 传统的数据共享模型往往依赖于可信的第三方中心化机构,但这种方案易发生单点故障,对参与方不透明,数据可能遭到篡改. 本文利用区块链能够去中心解决信任问题这一特点,提出一种基于区块链的物联网数据共享模型. 本文首先分析了现有的物联网数据共享模型以及 Hyperledger Fabric 区块链平台的关键组件,然后介绍了本文所述模型的网关组成方式和数据存储到区块链账本的内容,并对安全性和数据隐私性提出了增强改进设计方法,最后分析了模型的安全和可用性,通过测试简化模型的性能证明了模型实施的可行性.

关 键 词: 区块链; 物联网; Hyperledger Fabric; 数据共享
中图分类号: TP311 **文献标识码:** A **文 章 编 号:** 1000-1220(2019)11-2324-06

Data Sharing Model for Internet of Things Based on Blockchain

YU Jin-gang[1,2], ZHANG Hong[1,2], LI Shu[3], MAO Li-shuang[2], JI Peng-xiang[2]

[1](University of Chinese Academy of Sciences, Beijing 100049, China)
[2](Shenyang Institute of Computer Technology, Chinese Academy of Sciences, Shenyang 110168, China)
[3](Shenyang Ligong University, Shenyang 110159, China)

Abstract: With the development of Internet of Things technology, the structure of Internet of Things is becoming more and more complex, the amount of data collected shows explosive growth, thus how to safely share data between different participants has become a huge challenge. The traditional data sharing model is often dependent on the trusted third party centralized organization, but this scheme is likely to cause a single point of failure, is not transparent to participants, and data may be tampered with. To tackle this problem, we propose a data sharing model for Internet of Things based on blockchain, which uses the feature that blockchain can establish trust without any centralized organization. We first analyze the existing data sharing models of Internet of Things and the key concepts of Hyperledger Fabric blockchain platform. After that, the design of gateway and the content of data stored in blockchain ledger are illuminated, the enhancement methods of security and data privacy are proposed. Finally, the security and availability of the model are analyzed, and the feasibility of the model is proved by simplified testing.

Key words: blockchain; Internet of Things (IoT); Hyperledger Fabric; data sharing

1 引 言

伴随芯片、传感器及网络通信等技术的迅速发展,物联网(Internet of Things)产业体系初步形成,市场规模逐年扩大,设备数量呈现爆发式增长. 根据 GSMA 的报告,2017 年全球共有 75 亿台物联网设备,预计到 2025 年将增长至 250 亿,届时物联网市场价值将达到 1.1 万亿美元[1,2]. 面对日益增长的数据量和愈加复杂的网络拓扑结构,如何在不同的物联网组织间安全地共享数据成为了一个巨大的挑战. 一种典型的方式是引入可信的中心化机构,由该机构负责收集、传输和管理数据,但这种方案建设、维护成本高,对参与方不透明,且中心化机构易遭受恶意攻击,数据存在被篡改的风险.

区块链(blockchain)起源于比特币(Bitcoin)[3],是一种由多方维护、数据无法更改的分布式账本技术(distributed ledger technology, DLT),具有去中心化、共同维护、不可篡改、加密安全等特征. 它能够在脱离中心化机构的情况下使参与方建立互信,这一优势适合于改进物联网现有架构. 区块链通过共识(consensus)机制确保账本数据相同,任何参与者都无法绝对获得账本的控制权. 它将数据按时间顺序打包至区块,每个区块均包含前一区块的摘要信息,从而形成链式的形态,保证上链数据不被篡改和伪造. 区块链一般还包含智能合约(smart contract)或链码(chaincode),可以将规则或合同编码为程序

收稿日期: 2019-04-17 收修改稿日期: 2019-05-10 作者简介: 于金刚,男,1979 年生,博士,研究员,CCF 会员,研究方向为 IP 通信技术; 张 弘,男,1991 年生,硕士研究生,CCF 会员,研究方向为区块链技术; 李 姝,女,1985 年生,博士研究生,助理研究员,CCF 会员,研究方向为网络通信、人工智能; 毛立爽,男,1987 年生,硕士,CCF 会员,研究方向为 IP 通信技术; 姬鹏翔,男,1988 年生,硕士,研究方向为计算机应用技术.

部署到区块链上,触发条件后按事先的约定自动执行[4],以太坊(Ethereum)[5]是最早也是最著名的将区块链与智能合约相结合的应用平台.

按权限管理的不同,区块链一般分为公有链、私有链和联盟链. 公有链以众多加密货币为代表,其信息完全公开,任何人都可以自由进出网络,参与和维护账本. 私有链则与之相反,信息不公开,只有少部分人使用,由管理者统一管理,不同节点拥有不同的操作能力. 联盟链介于公有链和私有链之间,通常针对企业级应用,由利益不完全一致的参与方组成,各方之间存在一定的信任,但没有单一可信方,支持权限管理、身份认证[6,7]. 联盟链以基于 Golang 实现的 Hyperledger Fabric 为代表,它在设计上可插拔、可扩展,其共识机制、成员服务、加密算法、底层数据库等均可灵活替换,方便满足不同场景的使用需求.

本文以 Hyperledger Fabric 为基础平台,提出一种基于区块链的物联网数据共享模型. 该模型在不借助单一可信中心化机构的前提下,直接在参与方之间建立信任,保障数据能够安全共享.

2　相关技术

2.1　现有的物联网数据共享模型

在物联网中,属于某个组织的数据,可能对另一个组织的成员同样具有价值. 如果数据彼此独立存储与维护,不能流通,将形成数据孤岛. 为了解决这一问题,需要合适的数据共享模型.

一种方案是数据请求方与提供方间通过令牌等方式建立连接,直接进行数据传递. 但这种模型有几个严重的缺陷:

1) 数据的一致性无法保证. 如图 1 所示,当不同的请求方请求同一数据时,数据提供方由于故意或无意的原因,发送的数据可能是不同的,且难以被审计发现;

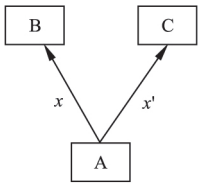

图 1　A 向 B、C 发送了不同的数据

Fig. 1　A sent different data to B and C

2) 接口格式不统一. 物联网具有很强的多源异构特性,每个数据提供方可能都有一套自己的接口方案,请求方要对这些接口分别做适配,处理起来十分复杂;

3) 数据提供方的负载过大. 数据提供方需要处理大量的请求,极易造成服务的不稳定乃至崩溃;

4) 安全防护脆弱. 数据提供方的安全防护能力各不相同,容易遭到攻击造成数据泄露,而严格的安防措施需要耗费大量人力物力.

另一种更普遍的方案是多个组织共同建立数据中心. 由于自建数据中心的成本大、维护难度高,因此当前多采用第三方云平台构建. 这一模型将数据交给集中式的云平台管理,数据的共享由云平台统一调度,效率大大提高,也不会出现数据不一致的情况. 但该模型也有一些问题[8]:

1) 传输延迟和资源浪费. 因为数据存储在云平台,即使请求组织内部的数据也要访问云端,长距离的传输将产生不必要的延迟. 如果在本地就近建立数据中心,又产生重复建设的问题;

2) 单点故障. 数据的读写依赖于云平台,网络结构的中心化对云平台的压力很大,一旦其出现故障,将导致系统瘫痪;

3) 安全和隐私保护. 将数据上传到云平台意味着其作为第三方有能力接触到数据,而这类中心化机构很多情况下并非完全可信,云平台的管理者或外部人员可能对数据进行篡改或泄露,破坏数据的完整性与机密性.

有鉴于此,研究安全高效的去中心化物联网数据共享模型具有重要的现实意义.

2.2　Hyperledger Fabric

Hyperledger Fabric 是一个提供区块链解决方案的平台,开发者能够在其基础上做进一步扩展. 它具有完备的权限和身份管理方案,注重交易安全和模块化设计. 其关键组件包括:

1) 客户端(Client):封装了区块链网络的底层接口,可以通过命令行或 Fabric SDK 调用,用于在应用和区块链网络之间进行交互. 客户端能够实现在网络中发起交易(transaction)、监听消息、更新配置、启停节点等功能.

2) 节点(Peer):包括背书节点(Endorser)和确认节点(Committer)两类. 背书节点对收到的请求按事先制定的策略(Policy)进行检查(例如,必须有属于组织 A 和组织 B 的背书节点同时批准交易的合法性),计算交易执行结果,如果符合要求则予以签名并返回. 确认节点负责向区块写入交易,更新账本的本地副本. 节点通常都具有确认功能,一部分节点具有背书功能.

3) 排序服务(Ordering Service):为收集到的合法交易按一定的时间顺序进行排序,再打包成区块数据广播至区块链网络. 排序服务所采用的共识机制是可插拔的,其去中心化程度可以自行选择.

4) MSP(Membership Service Provider,成员服务提供者):区块链网络中负责成员身份管理和认证的抽象组件. Hyperledger Fabric 中的成员通常从属于某个组织(Organization),多个组织最终结成了联盟. 而为了管理组织之间的关系及其成员的权限,MSP 定义了一系列颁发和校验数字证书的标准化规范,在节点、排序服务、通道等组件的配置文件中均包含被授权组织的 MSP 相关信息. Fabric CA[9]是官方基于 PKI 的 MSP 默认实现.

5) 链码(Chaincode):在其他区块链平台上也称作“智能合约”. Hyperledger Fabric 中提供了系统链码和用户链码,前者用于系统内部的管理和维护,后者用于提供对外部应用的可编程支持,通过执行代码逻辑与账本交互. 用户链码可采用 Golang、Java、Node. js 等通用编程语言编写,在节点的 Docker 容器环境中隔离运行.

6) 通道(Channel):可以认为是建立在区块链网络上的子网,能隔离交易,使得通道外部成员无法访问和修改通道内部的数据,实现区块链数据的权限管理. 每个通道都有自己的访问策略、组织身份及排序服务等.

3 基于区块链的物联网数据共享模型设计

3.1 模型总体设计

物联网架构可以分为四层[10]. 本文设计的模型在管理服务层利用区块链技术对数据的存储和使用方式做出了改进，取代了常见的数据中心，如图 2 所示.

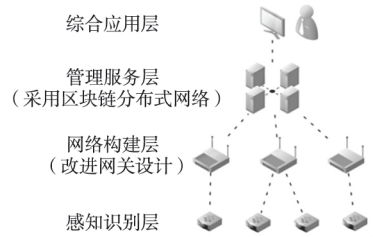

图 2 针对物联网架构的改进

Fig. 2 Improvement to the IoT architecture

基于此架构，本文提出基于区块链的物联网数据共享模型. 其总体设计如图 3 所示，在保留区块链自身优势的基础上，设计了一种新型网关，指定了多源异构数据存储到账本的内容，并在安全性和数据隐私性方面提出了几种增强设计方法.

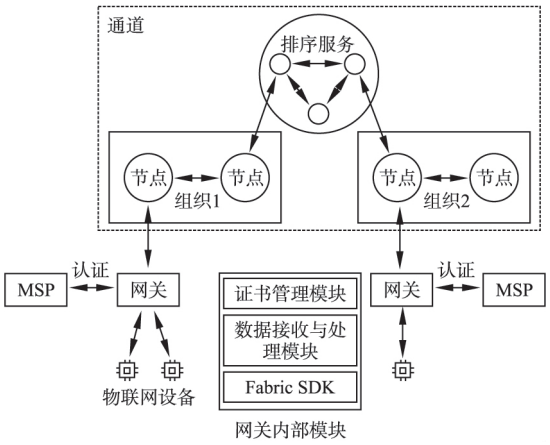

图 3 模型总体设计

Fig. 3 Model overall design

模型的主要特点包括:

1) 服务节点的网络拓扑去中心化，组织内部成员可以就近访问本地节点，节点彼此间高度自治，即使个别节点发生故障，系统整体仍然能够正常工作.

2) 由 MSP 提供安全灵活的权限管理方案，保证只有授权成员读写数据，数据在不同的参与方间可以被安全共享.

3) 数据由多个参与方共同维护，某一方对数据的篡改不会被系统整体所接受. 通过区块链共识机制同步数据，保证数据的一致性.

4) 链上数据以统一格式存储于账本，便于多方共享.

5) 可靠地保存数据访问记录，一旦发生数据泄露，通过分析这些记录可以追查到薄弱环节.

3.2 网关设计

物联网设备通常资源较少，存储和计算能力较弱，因此常常需要网关代为在网络上通信. 本文设计的网关由证书管理模块、数据接收与处理模块和 Fabric SDK 组成，三者相互配合令物联网设备与区块链网络实现交互. 其中，证书管理模块用于申请和存储物联网设备的证书; 数据接收与处理模块用于接收物联网设备采集的数据并对其进行处理; Fabric SDK 用于与区块链网络进行通信. 各模块的执行步骤如下:

步骤 1. 当新的物联网设备打算接入到区块链网络中时，由网关确认设备的身份，若通过，证书管理模块向对应 MSP 发送 HTTP POST 请求，申请注册该设备的身份证书.

步骤 2. MSP 收到请求后进行验证，如果合法，生成证书后返回给证书管理模块; 如果不合法，返回非法提示. MSP 事先已经在区块链网络中的通道、排序服务、节点等组件的配置中获得了授权，因此其颁发的证书等能够在网络中使用.

步骤 3. 证书管理模块收到证书后，将其加密存储于本地数据库，并记录证书与物联网设备的对应关系.

步骤 4. 数据接收与处理模块接收物联网设备采集的数据，对数据进行必要的清洗、格式转换等处理，并将处理后的数据交给 Fabric SDK.

步骤 5. Fabric SDK 使用物联网设备的证书进行签名，将数据封装成交易提案后发送到通道内的节点.

设备注册流程如图 4 所示.

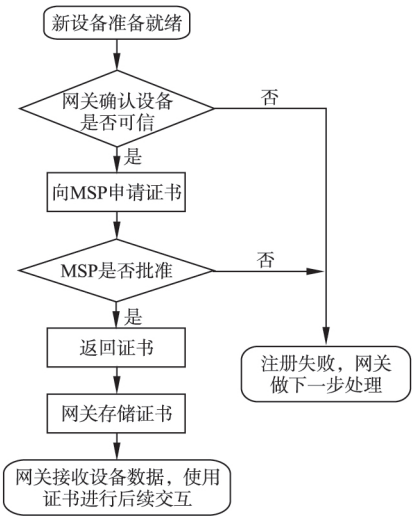

图 4 设备注册流程

Fig. 4 Device registration flow

此外，区块链网络中包含了各种各样的事件，如通道事件、区块事件、链码事件等，网关可以对关心的事件进行监听，从而基于事件采取下一步的操作.

3.3 账本内容设计

在账户模型上，Hyperledger Fabric 将账本大体分成了区块数据和世界状态(world state) 两部分. 区块数据在文件系统上存储，以不可篡改的方式记录了全部交易历史，数据只能增加不可修改. 世界状态存储于 Key-Value 数据库，状态值由区块数据的交易历史决定，可以被外部程序快速访问. 本文为世界状态设计了以下需要存储主要的内容，区块数据的交易应携带的内容可以从中推导得出.

首先，key 与物联网设备一一对应，其组成为:

< 设备所属组织 ID. 设备类型. 设备 ID >

其次,value 为一系列键值对,类似 JSON,数据提供方必需的字段如表 1 所示,其他未列出的字段可自定义.

3.4　安全设计方法

因为信任链(chain of trust) 的存在,现实中的数字证书大多由根 CA 授权的中间 CA 签署,既提高了签署效率,也有利于系统安全. 本模型的 MSP 也采用此种增强手段,使用分层结构签发证书,即不由根证书而是由根证书签发的中间证书来为所属组织的成员提供权限服务,根证书离线保存. 这样,即使某一 MSP 的私钥泄露,也只会对它所签发的证书造成影响,不会破坏其他 MSP 的安全性.

表 1　世界状态的必需字段

Table 1　Required fileds in world state

字段	说明
type	可以取 raw 或 hash. raw 代表后面 value 字段记录的是真实的原始数据,hash 代表 value 字段记录的是原始数据的散列值
id	设备 ID
status	设备状态,标识设备处于开启还是关闭等状态
lastUpdated	数据更新时间
value	记录的数据值,可以为数组,值的类型由 type 字段决定

出于安全需要,本模型将共享数据所写入的通道称为"数据通道",在此基础上提出"日志通道"这一概念. 数据通道不再直接提供查询接口,对数据的每一次查询都通过日志通道对数据通道链码的调用完成,进而可以在日志通道记录下查询项、查询者和查询时间等信息,如图 5 所示. 一旦数据通道的数据发生泄露,通过分析日志通道的记录,可以追查到薄弱环节和可能泄露的范围.

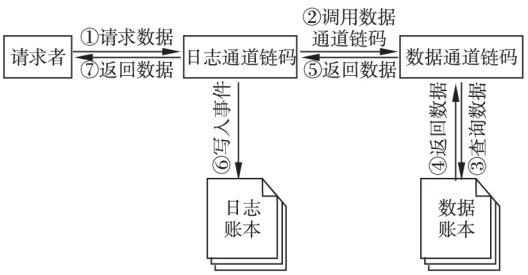

图 5　日志通道

Fig. 5　Log channel

3.5　数据隐私设计方法

在物联网的业务往来中,有时即使几个组织处于同一个区块链网络,也不愿意将自己的敏感数据公开给不相关的参与方. 为此,可以采取措施进一步保护数据的隐私性.

如果相关成员都完整参与了同一项业务,可以为这些成员新建单独的通道. 通道有自己的账本和访问策略,链上数据对通道内部成员可访问,对外完全隔离. 这是一种粗粒度的数据隐私保护方法.

如果需要部分数据公开,部分数据保密,对数据进行细粒度的保护,则采取以下方案. 在网关发送交易提案时,将隐私数据存储在特殊域中,背书节点识别到隐私数据,对其做散列计算,散列值返回给网关,隐私数据同步给其他授权节点,并存入本地数据库. 这样,散列值最终写入账本,隐私数据仅在授权节点存储. 当请求方希望访问隐私数据时,可以向节点请求,如果请求方被授予了权限,节点从本地读取或向其他存有数据的节点请求后将数据返回,请求方对收到的数据计算散列值,将该值与链上值做对比以确认数据的一致性. 此方法通过链上散列值完成了数据存在性证明.

当需要兼顾第三方监管时,又可采取以下方案. 对于某一物联网设备,它分别持有一对用于签名的密钥和一对用于加密的密钥. 签名密钥由网关在本地生成,私钥自己保存; 加密密钥由 MSP 生成,交给监管方备案. 网关所提交的数据通过加密公钥进行加密,签名私钥进行签名,存储于区块链上. 必要时,监管方可以使用加密私钥解密交易数据,以确认数据内容. 签名私钥则不做保留,防止身份被伪造.

4　分析及实验

4.1　安全和可用性分析

模型权限的安全性建立在 PKI 体系之上. PKI 体系广泛应用于计算机安全领域,其安全性已被有效证明. 区块链网络中的每一个操作几乎都有发起方的签名,其他组件可以利用对应公钥验证发起方的身份,只有被授权的操作才能执行. 而因为仅有发起方才知道它自身的签名私钥,不属于发起方的操作无法被第三方伪造.

模型继承了区块链防篡改的特性. 攻击者如果想篡改链上数据,必须控制区块链网络中的多数节点,而对于分布式网络来说这极为困难.

去中心化避免了单点故障问题,带来了可用性的提升,如图 6 所示. 不同组织维护了多个账本副本,即使单个节点发生故障或遭到 DDoS 攻击,系统也提供了继续工作的备选节点,不会对系统整体的稳定运行造成影响.

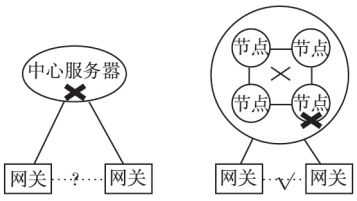

图 6　去中心化带来的可用性提升

Fig. 6　Increased availability from decentralization

4.2　实　验

本节实验部署了一个简化模型,用于测试模型性能. 测试环境如表 2 所示.

表 2　测试环境

Table 2　Test environment

CPU	2. 6 GHz Intel Core i5
存储	8 GB 内存,256 GB SSD
操作系统	macOS 10. 13. 6
软件	Hyperledger Fabric 1. 4. 0,Docker 18. 09. 1
账本数据库	LevelDB
测试脚本	Node. js

测试区块链网络运行在单台主机上,包含分属于 2 个组

织的 4 个节点、2 个 MSP,1 个采用 SOLO 共识的排序服务,5 个客户端,以上组件同属于 1 个通道. 测试方法为向区块链网络发送 5000 笔交易,交易类型分别为写入和查询,观察在不同的交易发送频率(Send Rate)下,系统的平均时延(Avg Latency)和吞吐量(Throughput)的变化. 结果如图 7、图 8 所示.

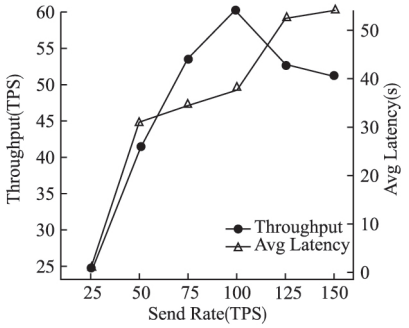

图 7 写入性能

Fig. 7 Open performance

可以看到,平均时延随着交易发送频率的提高均有上升. 吞吐量在写入交易发送频率为 100TPS(transactions per second,每秒交易数)、查询交易发送频率为 250TPS 时达到最大. 其中,写入吞吐量最高为 60TPS,这比公链上的比特币(7TPS)和以太坊(15TPS)要好,但远低于文献[11]测试达到的上千 TPS,分析原因在于文献[11]使用了高性能服务器运行各个组件,大大缩短了签名和加密等耗时操作的时间,而本节实验的所有组件都运行在资源有限的单机上.

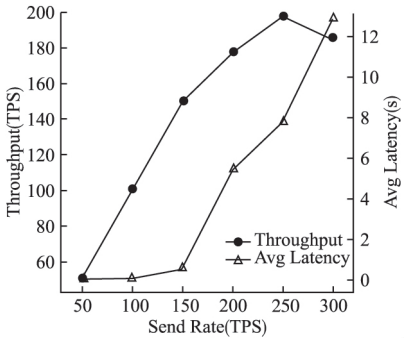

图 8 查询性能

Fig. 8 Query performance

尽管该区块链网络只包含 4 个节点,但由于背书策略(Endorsement Policy)的存在,仍然能保证网络是去中心化、防篡改的. 背书策略可以指定为不同组织和节点的组合,客户端必须收集到规定成员的一致背书才能提交有效交易,不存在控制交易产生的单一中心节点. 对数据的篡改会造成区块散列值的改变,通过比对不同节点的账本及交易签名可以快速找到篡改之处,而基于篡改数据的更新将因为背书策略的限制,使得不同成员的背书结果不一致,交易会被认定无效.

对写入吞吐量最大的一组测试,记录其资源消耗情况,如表 3 所示.

从表 3 可知,各组件所消耗的资源不高,在保证吞吐量和时延的前提下能够满足模型的实现. 还可以看出,用于背书和确认的节点所占用的资源较多,实际部署时应注加强此类组件所在服务器的性能.

表 3 资源消耗情况

Table 3 Resource consumption

组件名称	内存平均占用(MB)	CPU 平均使用率(%)	磁盘写入量(MB)
节点 1	211.3	29.44	32.7
节点 2	182.9	25.56	32.7
节点 3	184.5	28.44	32.7
节点 4	173.7	27.27	32.7
排序服务	37.0	13.36	23.1

5 相关工作

针对区块链与物联网的结合,国内外已经做了一些相关工作. 早期受限于区块链平台的单一性,研究局限于比特币网络. 例如,赵赫等人[12]提出一种基于区块链的采样数据保护方法,避免数据遭到人为篡改,但这种方案由于比特币价格的上涨,当前实施的经济成本已经过高.

随着区块链平台的大量出现,各种新的模型和架构相继被提出. 赵明慧等人[13]提出一种基于区块链的可信框架,用于解决物联网中存在的各种问题; 张俊等人[14]采用多种区块链描述和建模电力能源系统不同的属性,提出“区块链群”这一架构改进智能分布式电力能源系统; 任彦冰等人[15]将信任量化为新的考察模型,利用区块链实现信任数据的共享; Samaniego 等人[16]以区块链作为物联网的服务架构,验证了该架构在云和边缘设备上的性能; Ali 等人[17]提出一种去中心化物联网数据访问模型,用来保护数据隐私,并在以太坊和 IPFS[18]上进行了验证; Selimi 等人[19]将 Hyperledger Fabric 应用于无线 Mesh 网络,在多台树莓派设备上搭建节点,测试了其性能和瓶颈,验证了可行性.

6 总 结

本文以 Hyperledger Fabric 为基础平台,提出了一种基于区块链的物联网数据共享模型. 该模型设计了一种网关组成方式以及物联网数据存储到区块链的内容,并对安全性和数据隐私性提出了增强改进方法. 分析了模型的安全和可用性,通过测试简化模型的性能证明了模型实施的可行性. 借助本模型,不同物联网组织间的数据可以在不借助第三方中心化机构的情况下实现存储和共享,能够提高物联网数据传递的效率.

References:

[1] Sylwia Kechiche. Infographic: internet of things [EB/OL]. https://www.gsmaintelligence.com/research/2018/02/infographic-internet-of-things/654/,2019.

[2] GSMA. IoT report: how greater China is set to lead the global industrial IoT market [EB/OL]. https://www.gsma.com/iot/greater-china-industrial-iot-report/,2019.

[3] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. https://bitcoin.org/bitcoin.pdf,2008.

[4] Shao Qi-feng,Jin Che-qing,Zhang Zhao,et al. Blockchain: architec-

ture and research progress [J]. Chinese Journal of Computers, 2018, 41(5): 969-988.

[5] Ethereum Foundation. Ethereum project [EB/OL]. https://www.ethereum.org/, 2019.

[6] Yang Bao-hua, Chen Chang. Principle, design and application of blockchain [M]. Beijing: China Machine Press, 2017.

[7] Liu Ao-di, Du Xue-hui, Wang Na, et al. Research progress of blockchain technology and its application in information security [J]. Journal of Software, 2018, 29(7): 2092-2115.

[8] Zhang Jia-le, Zhao Yan-chao, Chen Bing, et al. Survey on data security and privacy-preserving for the research of edge computing [J]. Journal on Communications, 2018, 39(3): 1-21.

[9] The Linux Foundation. Fabric CA [EB/OL]. https://github.com/hyperledger/fabric-ca, 2019.

[10] Liu Yun-hao. Introduction to internet of things [M]. Beijing: Science Press, 2010.

[11] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains [C]//Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 2018, 30: 1-30: 15.

[12] Zhao He, Li Xiao-feng, Zhan Li-kui, et al. Data integrity protection method for microorganism sampling robots based on blockchain technology [J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2015, 43(S1): 216-219.

[13] Zhao Ming-hui, Zhang Lu, Qi Jin. A framework of trusted services management based on blockchain in social Internet of Things [J]. Telecommunications Science, 2017, 33(10): 19-25.

[14] Zhang Jun, Gao Wen-zhong, Zhang Ying-chen, et al. Blockchain based intelligent distributed electrical energy systems: needs, concepts, approaches and vision [J]. Acta Automatica Sinica, 2017, 43(9): 1544-1554.

[15] Ren Yan-bing, Li Xing-hua, Liu Hai, et al. Blockchain based trust management framework for distributed Internet of Things [J]. Journal of Computer Research and Development, 2018, 55(7): 1462-1478.

[16] Samaniego M, Deters R. Blockchain as a service for IoT [C]//2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 2016: 433-436.

[17] Ali M S, Doluik, Antonelli F. IoT data privacy via blockchains and IPFS [C]//Proceedings of the Seventh International Conference on the Internet of Things, Linz, Austria, 2017: 1-7.

[18] Protocol Labs. IPFS is the distributed web [EB/OL]. https://ipfs.io/, 2019.

[19] Selimi M, Kabbinale A R, Ali A, et al. Towards blockchain-enabled wireless mesh networks [C]//Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Munich, Germany, 2018: 13-18.

附中文参考文献:

[4] 邵奇峰,金澈清,张 召,等. 区块链技术: 架构及进展 [J]. 计算机学报,2018,41(5): 969-988.

[6] 杨保华,陈 昌. 区块链原理、设计与应用 [M]. 北京: 机械工业出版社,2017.

[7] 刘敖迪,杜学绘,王 娜,等. 区块链技术及其在信息安全领域的研究进展 [J]. 软件学报,2018,29(7): 2092-2115.

[8] 张佳乐,赵彦超,陈 兵,等. 边缘计算数据安全与隐私保护研究综述 [J]. 通信学报,2018,39(3): 1-21.

[10] 刘云浩. 物联网导论 [M]. 北京: 科学出版社,2010.

[12] 赵 赫,李晓风,占礼葵,等. 基于区块链技术的采样机器人数据保护方法 [J]. 华中科技大学学报(自然科学版),2015,43(S1): 216-219.

[13] 赵明慧,张 琅,亓 晋. 基于区块链的社会物联网可信服务管理框架 [J]. 电信科学,2017,33(10): 19-25.

[14] 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.

[15] 任彦冰,李兴华,刘 海,等. 基于区块链的分布式物联网信任管理方法研究 [J]. 计算机研究与发展,2018,55(7): 1462-1478.