基于双区块链的基站动环信息监控系统

樊建峰[1,2] 李 轶[1] 吴文渊[1] 冯 勇[1]

(中国科学院重庆绿色智能技术研究院自动推理与认知重庆市重点实验室 重庆 400714)[1]

(中国科学院大学 北京 100093)[2]

摘 要 基站动环监控系统通过将基站智能监控单元构建在底层被监控的智能和非智能设备之上,实现全网基站动环信息的监控、实时告警等功能。因此,动环监控系统的稳定是安全运行的前提。但随着基站数量的增加,现阶段中心服务器架构模式下的系统会显现出负载增加、流量过载等问题,且多对一的模式下容易出现 DoS 攻击、数据泄露等安全问题;另外,在多用户模式下,现有的系统模式无法达到对细粒度访问权限的控制。针对上述问题,结合区块链技术在分布式架构上独特的优势,文中提出一种基于改进型 PBFT 共识算法的双区块链基站动环监控系统架构,来解决现有动环监控系统中心化、安全、扩展等问题。具体地,该系统是一种层次型架构的信息系统,且各层次各维护一条区块链,是一个多节点共同维护与共享的双链区块链系统。其中,一条以联盟链的形式负责跨域信息的流转和权限的控制,另一条以私有链的形式负责基站设备访问权限的控制以及基站事务信息的流转。同时,基于 PKI 系统和密钥管理系统的支持,以及改进型区块头对权限信息的存储,达到对设备的细粒度访问权限的控制。最后,定性分析的结果表明了,相较于现有的传统动环监控系统,文中系统具有多中心服务、抗 DoS 攻击、基于用户的细粒度权限管理、信息的加密完备程度高和扩展性好等特点。

关键词 基站动环监控系统,区块链,分布式系统安全,PBFT 共识算法,权限控制

中图法分类号 TP315 **文献标识码** A **DOI** 10.11896/jsjkx.190300041

Double Blockchain Based Station Dynamic Loop Information Monitoring System

FAN Jian-feng[1,2] LI Yi[1] WU Wen-yuan[1] FENG Yong[1]

(Chongqing Key Laboratory of Automated Reasoning and Cognition, Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences, Chongqing 400714, China)[1]

(University of Chinese Academy of Sciences, Beijing 100093, China)[2]

Abstract The power and environment monitoring system of base station realizes the functions of the whole network base station power and environment monitoring and real-time alarm by constructing the base station intelligent monitoring unit on the underlying intelligent and non-intelligent devices. Therefore, the stability and safe operation of the power and environment monitoring system is a prerequisite. However, as the number of base stations increases, the system in the central server architecture mode will show problems such as increased load and traffic overload, and the many-to-one mode is prone to DoS. Security issues such as attacks and data breaches. In addition, in multi-user mode, the existing system mode cannot achieve fine-grained access control. Aiming at the above problems, combined with the unique advantages of blockchain technology in distributed architecture, this paper proposed a double blockchain power and environment monitoring system of base station architecture based on improved PBFT consensus algorithm to solve the centralization, security, expansion and other. of the existing system problems. Specifically, the system is a hierarchical architecture information system, and each layer maintains a blockchain. the system is a dual-chain blockchain system that is maintained and shared by multiple nodes. One is responsible for the flow of cross-domain information in the form of a league chain, and the control of the authority, the other is responsible for the access control of the base station device and the flow of the base station transaction information in the form of a private chain. And achieves fine-grained access control of the device through PKI system and the key management system, and the improves block header to store the permission information. Finally, the results show that compared with the existing traditional system, the system of this paper proposed has certain advantages of multi-center service, anti-DoS attack, user-based fine-grained rights manage-

到稿日期:2019-03-13 返修日期:2019-07-24 本文受国家自然科学基金项目(61572024),重庆市自然科学基金(cstc2019jcyj-msxmx0638),重庆市院士牵头科技创新引导专项(cstc2017zdcy-yszxX0011,cstc2018jcyj-yszxX0002)资助。

樊建峰(1993—),男,硕士生,CCF 会员,主要研究方向为信息安全、区块链,E-mail:fanjianfeng17@mails.ucas.edu.cn;**李 轶**(1980—),男,副研究员,硕士生导师,CCF 会员,主要研究方向为程序验证、符号计算、信息安全,E-mail:zm_liyi@163.com(通信作者);**吴文渊**(1976—),男,研究员,硕士生导师,主要研究方向为同伦计算、信息安全;**冯 勇**(1965—),男,研究员,博士生导师,主要研究方向为数值混合计算。

ment, high degree of information encryption and good scalability through the qualitative analysis.

Keywords Power and environment monitoring system of base station, Blockchain, Distributed system security, PBFT consensus, Access control

1 引言

随着经济的发展,通信行业的发展也表现出了强劲的势头,从 3G 到 4G 再到 5G 技术,通信越来越便捷。通信行业的快速发展,也带动了支撑其发展的基础设施产业的日益繁荣,尤其是为了保证通信的质量和基站的安全,其规模被迅速扩大。为了保证基站的正常运行,相关公司加大了在基站运维方面的投入。2014 年 9 月,国内通信基础设施建设相关公司共同组建了中国铁塔股份有限公司,用于对基础通信设施进行统一建设和管理。基站动环监控系统便是其中的一个重要配套系统,该系统主要用于对基站、机房等运行环境数据进行远程监控,当前广泛采用的是"互联网+,大平台"+"智能监控单元(FSU)"的模式。基站动环监控系统通过将基站智能监控单元构建在底层被监控智能和非智能设备之上,实现对全网基站动环信息的监控和实时告警[1]。

目前,国内的基站监控系统也比较多,比如中兴、华为、大唐电信公司等,其中具有代表性的是中兴的 E-Guard 基站监控系统[2]。国外最大的制造商位于美国,即艾默生网络能源有限公司,其设计开发的动力环境监控系统在国内的应用也较为广泛。传统基站监控系统多采用图 1 所示的中心系统架构。

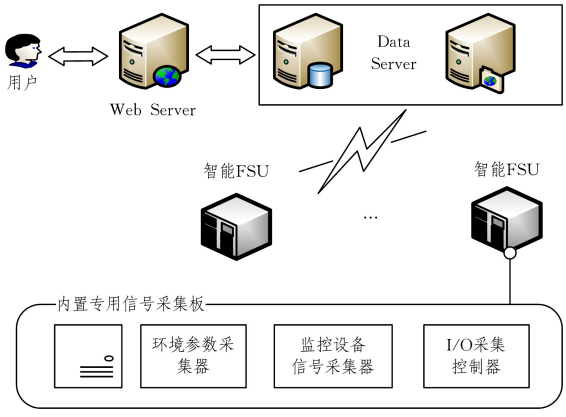

图 1 传统基站监控系统架构

Fig. 1 Traditional monitoring system of base station architecture

动环监控系统主要的应用商,即三家电信企业(移动、联通、电信),从原有的动环监控单元(SU)到中国铁塔股份有限公司的基站智能化监控单元(FSU),终端侧对数据的处理能力得到了显著的提升,在一定程度上减缓了平台侧服务器的压力[1,3]。但不变的是,现有的动环监控系统依旧采用的是中心化的集约数据处理和派单架构服务模式。该模式下存在诸多问题,这也成了监控系统发展的桎梏所在。

1)随着基站数量的增多,服务器平台侧面临的负载也会增多,流量过载问题亦会日益凸显;在中心化的服务模式下,服务器容易出现单点故障,导致系统失效;另外,由于通信基站多位于室外,基站的物理安全难以得到保障,因此,在某些特殊情况下,其可能会成为黑客实施 DoS 等网络攻击的目标,为系统留下安全隐患。

2)现阶段基站复合性(多表现为多家运营商公司、各个运维公司共同享有该基站)使用越来越多,涉及到的公司、人员较多,导致基站的运行环境信息、动力系统以及门禁和特定区域的授权管理较为混乱。简而言之,当前的动环监控系统无法实现对各个设备权限的细粒度控制。

3)基站智能监控单元对各类智能或者非智能设备信息的采集和各类设备进行 I/O 操作的历史记录信息被暂存于 FSU 本地且无加密,因此容易造成泄露和丢失,无法确保历史数据的完整性、可追溯性。此外,各类系统所传输的敏感信息(如 I/O 操作信息等)也未实现完整的加密传输,带来了信息泄露的风险。

综上所述,现阶段使用的动环监控系统在服务架构层面、权限管理层面、信息的安全传输层面都存在很大的不足与隐患。因此,工程界迫切需要一种能够实现各参与单位间信息的共享和告警,并且能够保证信息的完整性和机密性以及整个系统的稳定性和健壮性的方案,而区块链技术为实现该目标提供了可能。

比特币(Bitcoin)[4],是 Nakamoto 于 2008 年推出的世界上第一个数字货币,而区块链(BlockChain,BC)便是比特币最主要的底层技术。它是一种按照时间顺序将数据区块以链条的方式组合形成的特定数据结构。区块链并不是一项单一的技术创新,而是 P2P 网络技术[5]、非对称加密技术[6]、共识机制[7]、链上脚本[8]、PoW 共识协议[9]等多种技术与密码学深度整合后实现的分布式账本技术[10]。基于区块链全网节点验证的共识机制、非对称加密技术以及利用 P2P 技术分布式存储数据等特点,既大幅地降低了黑客攻击的风险,也为共享式物联网解决现有的分布式管理和安全隐私等难题提供了可能性。区块链技术的具体特点如下。

1)去中心化:区块链缺乏中心控制节点,是通过所有参与 p2p 网络的节点来维持架构的良好运行,既消除了多对一的通信模式的弊端,也保证了架构的可伸缩性和健壮性,并且克服了单点故障等问题。

2)权限管理:区块链系统提供的密码学组件,为实现基站设备的细粒度权限管理提供了可靠的基础。

3)安全性:区块链技术利用各类密码学算法提供了一个安全的、去中心信任化的信息通信和存储环境,使信息传输的泄密问题和信息篡改问题得到了很好的解决。

但是,现有的区块链架构模型,譬如比特币[4]、以太坊[11]、超级账本[12]等,不适合直接用于该基站动环监控系统场景。因此,本文首次提出一种适用于基站动环监控系统的轻量级、去中心化、基于 PBFT 共识算法的双区块链架构,其具有易扩展、抗 DoS 攻击、基于角色控制的细粒度权限管理以及完备的信息加密等特点。文中对其安全特性和优越性进行分析,并对其未来的发展趋势进行了展望。

2 相关知识

2.1 密码学技术

密码学是区块链系统的重要组成部分,是实现区块链技

术的基础。区块链系统中主要涉及的密码学技术有 Hash 算法与数字摘要技术、加解密算法、数字签名、数字证书和 PKI 体系等。

Hash(哈希或者散列)算法能够将任意长度的二进制明文映射为固定长度的二进制串(Hash 值)，并且不同的明文几乎不可能映射为相同的 Hash 值。常见的哈希算法有 MD5[13]，SHA1[14]，SHA2[14] 等。数字摘要是对数字内容进行 Hash 运算，以获取唯一的摘要值来指代原始的完整数字内容。

加解密算法是密码学的核心技术，从设计理念上可以分为对称加密和非对称加密两种类型。对称加密算法指的是加解密所使用的密钥是同一个密钥。非对称加密算法即加解密使用不同的密钥进行运算，其缺点为运算较慢，代表性算法有 RSA，ECC，SM2 等系列算法。

数字签名是利用非对称加密算法对消息进行计算得到签名，而对签名进行验证，则可验证消息的完整性和签名归属性。常用的签名算法有 RSA[15] 签名方案、椭圆曲线签名方案[16] 和知名的数字签名算法 DSA[17]。

数字证书是一种对公钥进行保护和背书的技术，证书需要由证书认证机构(Certification Authority，CA)来进行签发和背书，以确保证书的权威性和有效性。CA 是 PKI(Public Key Infrastructure)系统的重要组成部分，其中系统主要包括 RA(Registration Authority)，KMC(Key Management Center)和 CRL(Certificate RevocationList)，它们主要负责对数字证书的验证发放以及密钥的管理和失效证书的维护。在基站动环监控系统中引入 PKI 体系，主要对参与动环监控系统的管理公司维护公司以及参与系统的用户的身份进行管理，以确保区块链系统中信息的完整性与不可抵赖性；另外，PKI 体系的引入，使得其可以运行于集团公司，对区块链的准入进行管理，引入一定的中心化管理，确保了系统的稳定性；其次，业务方面等信息的处理会被存入区块链系统，中心化的操作不会对业务数据的真实性和完整性产生影响。

2.2　实用拜占庭容错算法算法

实用拜占庭容错算法(Practical Byzantine Fault Tolerance，PBFT)[18] 是 Miguel Castro 和 Barbara Liskov 于 1999 年提出的一致性算法，该算法用于解决拜占庭容错算法不高效的问题。相较于原始拜占庭容错算法，该算法的复杂度由指数级降到了多项式级，因此其在分布式系统中得到了广泛的应用。

PBFT 算法是一种状态机副本复制算法，每个状态机的副本都保存了服务的状态，同时也实现了客户端所有合法请求的操作，能够在保证系统有效性的前提下，允许$\left\lfloor\frac{n-1}{3}\right\rfloor$个节点出错，其中 n 为分布式系统中所有参与共识过程的节点数量。

在 PBFT 共识的分布式系统中，节点有主节点和副节点之分。主节点用来接收客户端发送的请求消息，副节点是备份节点。

该算法达成共识包括 3 个阶段：预准备阶段、准备阶段和提交阶段。一个主节点收到客户端的请求以后，将会自动向其他副节点广播该请求。预准备阶段和准备阶段的存在可以给相同的 View 请求进行排序，规范了请求的执行顺序；准备阶段和提交阶段的存在可以对跨 View 请求进行排序。在没有错误节点的情况下，算法的执行如图 2 所示。

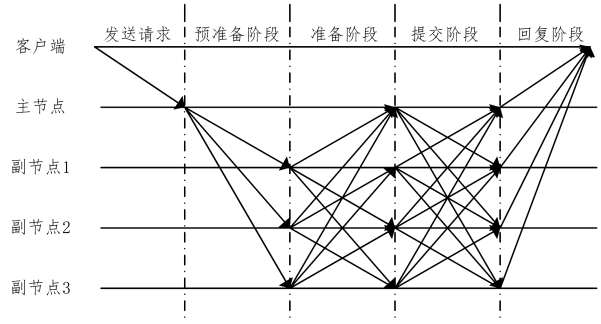

图 2　PBFT 算法流程图

Fig. 2　Algorithm flowchart of PBFT

3　基于 PBFT 算法的分布式区块链动环监控系统

区块链动环监控系统主要包括基站区块链智能监控单元 BCFSU(BlockChain Field Supervision Unit)、覆盖网络(Overlay Network)、共享型区块链系统(Shared BC) 3 部分。BCFSU 指的是基站信息采集和智能控制单元，负责基站各类接入设备的信号采集和处理，以及部分设备的 I/O 信号的转发操作；覆盖网络指的是区块链系统中各个记账节点以及接入节点所组成的网络；共享型区块链系统是运行于覆盖网络的区块链系统。系统整体结构如图 3 所示。

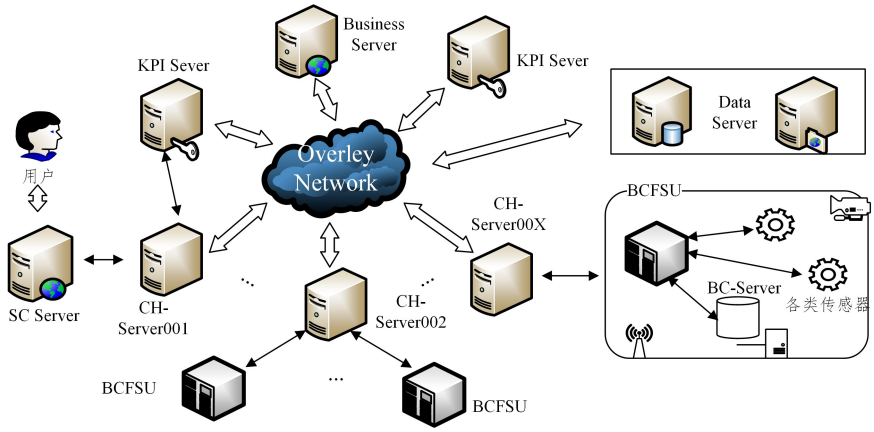

图 3　系统的整体结构

Fig. 3　System overall structure

3.1 基站区块链智能监控单元系统

BCFSU 系统的主要功能包括硬件端口信息采集和硬件 I/O 端口的控制、权限管理、存储管理、通信管理 4 个部分。

3.1.1 信息的采集和 I/O 控制

BCFSU 的信息采集主要包括机房的环境量(如温度、湿度等信号)、网管动力设备(如开关电源、空调等)、视频监控设备(重点机房)等。其中,部分信号需要系统采用轮询的机制进行获取,且将超出阈值的信号量及时地转发给上层的应用层,及时告警。

信息系统根据网络信息信号量,对与 BCFSU 连接的动力和门禁设备进行 I/O 控制,并对所控制的设备的状态量进行实时的收集和反馈。

3.1.2 权限管理

权限管理功能是基站动环监控系统非常重要的一部分。BCFSU 作为终端侧的基础设备,是基站信息采集和控制的载体,其安全性直接关系到整个系统的安全。因此,BCFSU 的权限管理主要涉及用户访问管理权限和设备通信权限管理两方面。

3.1.3 存储管理

本地区块链系统(Local BlockChain)的存储管理主要包括区块、交易单(Transaction,Tx)和非结构化等文件的存储管理,是动环监控系统最基本的构成部分。本地区块链的区块结构如图 4 所示。

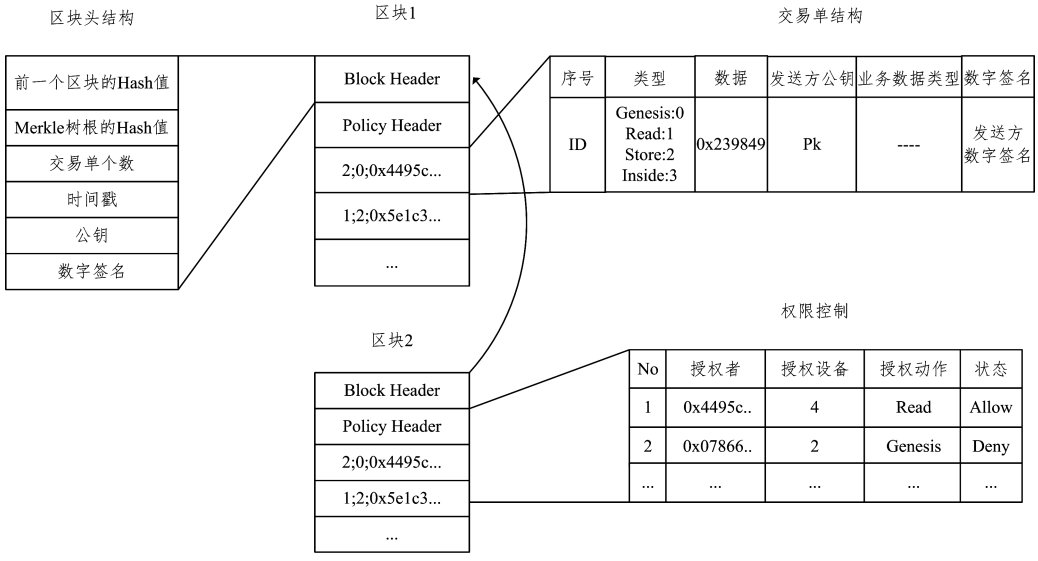

图 4 本地区块链系统区块及交易单结构

Fig. 4 Structure of block andtransaction of Local BC

本地区块链系统的区块结构由区块头(Block Header)、权限控制头(Policy Header)[19]和区块体(Block Body) 3 部分组成。一条区块链由一个个区块通过“链式”连接在一起,而每个区块又包含了若干交易单,交易单构成区块体,每个交易单是系统中一条业务数据的载体,它们通过交易单的形式打包进区块,以实现对业务数据流转的记录存储。

如图 4 所示,每个区块的区块头,包含前一个区块的 Hash 值、由交易单 ID 生成的 Merkel 树根哈希值、交易单个数、生成区块的时间戳、生成区块者的公钥以及对区块头进行签名的数字签名。通过区块头的 Hash 值,将每一个区块与前一个区块链接在一起,确保了区块数据不可修改的特性,也保障了数据的时序性。由于该区块链是本地链,因此其记账权限仅为服务节点自身,其业务需求仅为对机房流转信息的记录,故不存在像比特币一样的“挖矿”过程。

对于权限控制头,从区块链功能上区分,区块头是用于确保区块链信息安全性和完整性的结构,而权限控制头用于为动环监控系统中机房设备的细粒度权限控制提供数据结构基础,该数据结构包括序号、授权者、授权动作、授权设备、状态等信息。授权者包括但不限于授权给单个实体用户或者授权给具体用户组。授权动作根据业务需求,包括:Genesis,即对机房设备以及其他阈值等进行更新的交易类型;Read,即数据请求获取;Store,即数据的上传类型。授权设备为机房中各种机房数据设备的编号,授权动作为允许或者拒绝。

对于交易单,机房本地区块链的交易单按照动作类型分为 4 种:Genesis 类型,主要为对机房各阈值等信息的更新,以及设备固件的更新等;Inside 类型,主要为机房自身系统信息流转交易单;Store 类型,主要为机房数据上传交易单;Read 类型,主要为其他节点访问机房数据请求交易单。交易单的其他字段为交易单 ID,该 ID 为对交易单这个数据结构进行 Hash 运算的哈希值。哈希算法和编码算法可以选择 SHA-256 哈希算法[20],其可靠性已经在其他区块链系统中得到验证,尤其是比特币系统。数字签名为本交易单发起者的签名,亦确保交易记录的不可抵赖性。设备的 ID 为本交易所操作或者请求的设备 ID(实际请求中可由机房 BCFSU 根据业务需要进行指派),数据字段为本交易所传输的数据字段,若为非结构化数据,可以填写数据的 Hash 值,此种类型的交易单多为外部请求视频数据,当然亦可作为备用以供系统后期扩充所用。公钥字段为本交易单发起者的公钥。

此外,机房 BCFSU 除了维护本地区块数据库,还需维持一个本地文件数据库,主要用于对非结构化数据进行存储,如历史视频信息的存储等。采用 KV 型数据库,可以仅将数据的哈希值上链存储,将数据另存于文件数据库中,以此来降低区块链链上数据的膨胀,亦方便后期对其进行存取。

3.1.4 通信管理

BCFSU 的通信管理主要分为两种情况。当作为机房

BCFSU 角色时，其功能包括机房动环信息的采集和控制、权限的控制管理、内部数据的流转和服务、CH(ClusterHead)节点的选举服务等；另外需要特殊说明的是，当 BCFSU 作为 CH 节点服务器时，其不仅具有上述机房 BCFSU 角色的通信管理功能，还具有 CH 节点的通信管理功能，主要包括区块打包和验证功能、共识机制功能等，详细介绍请参见 3.3 节。

3.2　覆盖网络

覆盖网络是一个类似于比特币种的 P2P 网络，由各 CH 节点服务器、云存储服务器、KPI 服务器及其他服务器组成。为了降低网络的负载和延迟，各 BCFSU 在网络中以集群(Cluster)的形式存在，每个集群包括若干 BCFSU 或者其他服务器(Web 服务器等)，可以根据业务需求的设定或者网络负载等情况选举出一个 CH。CH 参与整个覆盖网络共享型区块链系统的事务，包括监听各节点的交易请求，打包和验证交易，以及同步其他区块和存储数据于云存储系统。集群中的节点可以在业务需求规定内，根据流量负载或者网络延迟等因素自由更换所在集群[19]。

每个 CH 节点包含一个集群节点信息列表。集群节点信息列表是指每一个集群所包含的 BCFSU 的节点信息(PK 和 IP 等信息)以及其他形式的接入服务器。该信息列表由 CH 节点维护，任何加入该集群的服务器或者 BCFSU 都需在该服务器认证注册，并由 CH 节点向 PKI 系统进行证书验证，且 CH 可及时发现脱离集群以及不合法的节点，并进行更新。

3.3　共享型区块链系统

共享型区块链系统，主要是指运行在覆盖网络的区块链系统。区别于本地区块链系统，共享型区块链系统主要负责跨系统业务信息的流转，其区块链节点包括各 CH 以及其他接入的功能型服务器。

3.3.1　区块的结构

如图 5 所示，共享型区块链系统的区块结构包括区块头和区块体。区块头包括前一个区块的 Hash 值、由交易单 ID 生成的 Merkle 树根哈希值、交易单个数、生成区块的时间戳以及对区块头进行签名的数字签名，结构与本地区块链系统结构类似，各字段功能也相同。区块体是由各交易单构成的，交易单结构如图 5 所示。其中，相较于 Local BC 的交易单，该交易单新增两个字段，分别为服务提供者 Pk 以及请求业务数据类型(根据实际业务，该字段可为空)，另外删减设备 ID 字段。服务提供者 Pk 主要用于 CH 检查集群节点信息列表，CH 节点监听到属于自身集群的服务提供者 Pk 时，则对该交易权限进行初步检查，若检查通过，则将该交易转发到相关的 BCFSU 进行处理。

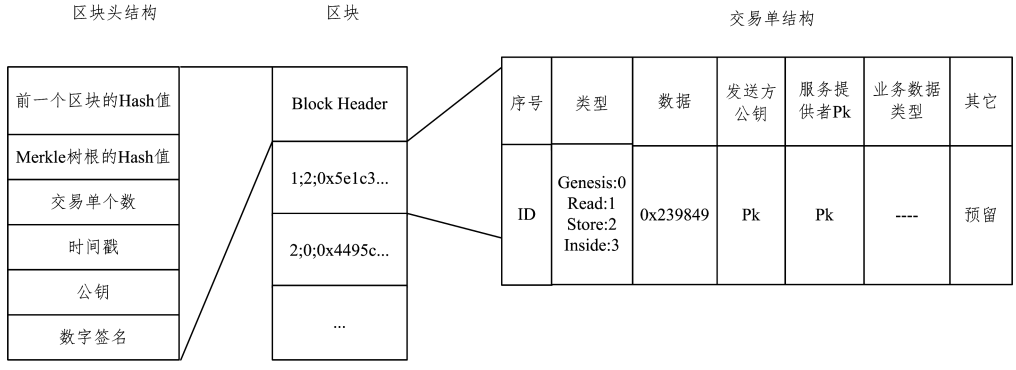

图 5　共享型区块链区块及交易单结构

Fig. 5　Structure of block and transaction of shared BC

3.3.2　节点管理

一个区块链系统节点最主要的功能有验证交易和验证区块正确的验证功能，以及生成交易单的生成功能和打包区块的打包功能，它们在共识算法的规范下协作运行。比如，对于比特币，节点根据交易生成交易单并对其进行签名，然后将交易单消息广播到区块链 P2P 网络中，参与其中的挖矿节点将对交易进行验证，验证通过则对其进行打包，通过共识算法生成区块，并将生成的区块广播到其他节点，其他节点对该区块和区块中打包的交易进行验证，验证通过则将该区块链接到本地区块链上。类似地，本系区块链系统的节点也有生成交易单、打包成区块、验证区块以及交易的功能。

一般来说，联盟区块链系统节点间以 PBFT 算法作为共识算法，能很好地避免 PoW 等工作证明的共识算法存在的能源浪费问题，亦不如 PoS 算法或者 DPoS 算法那样需要代币作为权衡节点记账权的标准，且能允许系统在少于$\frac{n-1}{3}$个节点因断电或者被劫持而无法正常工作等情况下继续良好运行，具有很好的工业应用性。此外，该算法亦能使系统的信息吞吐量达到很好的效果。

但是，对于该系统需要进行共识的 CH 记账节点，在集群流量过载或者失效等情况下，集群 BCFSU 会重新选举该节点。由于动环监控系统业务流量较为稳定，因此在整体节点保持稳定的情况下，仍会有部分 CH 节点会动态退出或者加入，但不会是大面积的。面对此种情况，若采用 PBFT 静态协议，动态节点的出现会导致系统重启，对系统的运行造成较大的影响。

因此，本文采用改进型 PBFT 算法[21]，其在保持 PBFT 算法优点的情况下，将 PBFT 算法的三阶段消息共识优化为两阶段，减少了网络开销和时间开销；且加入节点的生命周期，使得 PBFT 转变为动态结构而更加适用于存在动态节点的联盟链。动环监控系统作为一种多方参与的区块链系统，参与到区块链系统中的各方都由统一的集团 KPI 系统进行认证，且区块链系统中无论是本地区块链系统还是共享区块链系统都有严格的用户权限管理，对系统的稳定性和安全性起到了至关重要的作用。此外，由于共享型区块链系统提供

了多中心化的服务器数据管理功能,因此每个 CH 节点服务器均可被视为一台传统架构上的中心服务器,其他业务型服务器(如派单运维系统、工单上站处理系统、集团统一监控平台等)都可以直接加入到覆盖网络的区块链系统中,或者接入某一 CH 节点服务器进行业务操作或者数据的获取。该方案从架构上减轻了传统架构中中心服务器的压力,亦避免了因中心服务器宕机而导致的监控系统瘫痪。

另外,PBFT 算法的集群中各个 CH 服务器地位平等,且不存在中心化下因某方数据问题而导致的数据丢失、错误甚至被篡改等现象,使得信息的完整性、不可篡改性得到了保障,因此 PBFT 算法十分适用于该基站动环监控系统。

目前该领域还没有采用 PBFT 算法的先例,本文创新性地将 PBFT 算法应用于此。

3.3.3 数据存储

共享型区块链系统的数据存储与本地区块链系统的数据存储并无二致。

业界对动环监控系统数据接口传输的要求分为监控中心 SC 向 FSU 获取数据(慢数据),如温湿度、电压、电流、电量、频率、开关状态等,其中慢数据里的视频图像文件可以采取 FTP 的方式获取;FSU 主动上报设备数据(快数据),如告警、状态切换等。但是,出于对区块链系统性能的考虑,结构化数据可以生成交易单信息打包上链,而非结构化数据上链的成本过大,且传输上对网络环境要求较高,因此与本地区块链系统设计相同,可将所要传输的非结构化数据取哈希值添加到交易单中,且将原始数据存放于云存储系统。

云存储系统采取 Level DB 等 KV 型数据库,选用该数据的优势在于:相较于 MySQL 和 Oracle 等关系型数据库,此种非关系型数据库是一种通过键值对进行存储的、具有很好读写性能的数据库。对应于本文所述的非结构化数据的存储,可以将非结构化数据的哈希值作为 Key 键进行存储,以便于后期将交易单数据和非结构化数据进行快速的对应,使得系统有很好的性能。

3.3.4 区块的生成和验证

在 3.3.2 节中提到的改进型 PBFT 共识算法下,共识 CH 节点中会有节点被选举为主节点(记账节点),其负责对交易进行验证并打包生成区块,其他节点为副节点,负责对生成的区块进行验证上链。此节主要对主节点的验证记账过程和副节点的验证执行上链过程进行详解。

主节点收到来自其他副节点或者自治域内的集群交易时,对该交易单信息以及交易单的数字签名信息进行合法性校验,如果校验通过,还须对交易单的请求进行合法性校验。比如,交易单信息显示为某一运维公司请求该主机节点下辖某一基站的温度值信息,此时,主机节点需要根据其数字证书信息对其访问该基站信息是否合法进行校验,若校验合法,则接受该交易,并将其放入内存待打包列表。当待打包列表到达等待时间时,主节点将一定数量的交易单生成 Merkle 树,按照区块链打包规则将其打包成区块。此时主节点生成预准备消息,将该区块消息加入预准备消息,且广播给其他副节点,经过改进型 PBFT 的两阶段之后,各节点接受该区块,并将该区块链接到上一个区块,从而形成共识。区块共识的两阶段过程如下。

1)主节点根据校验完毕后的交易单生成新 m 区块,分配编号 n,然后向所有的节点广播快提案消息〈〈*FAST-PROPOSAL*,v,n,s,d〉,m〉,其中 s 为主节点签名,d 为消息摘要,m 为消息内容。

2)各副节点收到该消息后,对该消息的合法性进行校验,比如数字签名、格式等,若通过,则验证 v 和 n 是否在其他消息中出现过,但其签名不是主节点的信息。此外,还须验证 n 是否在水线的上限 h 和下限 H 之间,无误后保存,并根据提案消息生成快确认消息〈*FAST-CONFIRM*,v,n,s,d,i〉〉(其中 i 为自身编号),并对其进行签名,广播到除自己之外的所有节点。

3)各节点收到提交的信息后同样进行步骤 2)的合法性检查,验证通过后进行保存。当副节点接收了 $2f+1$ 个的编号 v 和预准备序号 n 相同而 IP 不同的提交消息以后,该节点截获该消息中的区块信息,并对该区块中包含的交易信息进行检查,若有属于本节点发送的交易,则将待确认列表中的交易删除;若发现交易中的请求服务方为本节点下辖的 BCFSU 地址(一般为公钥/或者公钥的哈希值)或者其他服务器的地址,则对该交易中的请求进行合法性检查,检查通过后将其重新打包转发,交由相应服务器处理。检索完所有交易后,该节点将该区块链接到上一个区块后,从而达成共识。

通过上述过程,可以保证在某一共识过程中出现恶意或者故障的节点小于或等于$\frac{n-1}{3}$时,共识过程依然可以正常完成[21]。在其他区块链系统中,类似于比特币,节点分为轻量级节点或者全节点。同样地,本文所述的共享型区块链系统中的节点亦分为全节点和轻量级节点,可以根据业务需求进行设定,若其他接入动环监控系统中的服务器仅为了对各类基站数据进行监控展示,即为轻量级节点,其不参与打包挖矿的过程,只对节点区块链和云存储服务器进行访问。因此,可以根据业务需求对服务器节点角色进行灵活配置。

3.3.5 用户与权限管理

从基站动环监控系统的业务层面来看,动环监控系统的参与实体大致可以分为 3 类:基站拥有者的基站管理公司、基站业务共享的运营商公司、基站运维的运维公司。基站管理公司按照业务可分为各省、地、市级公司,该公司基站实际的建设和拥有方对基站具有所有权,拥有高级管理权限。运营商公司主要共享基站管理公司的基站机房,对自己业务设备具有独占权力,但是对于基站公共动环设备仅根据业务需求,可以向基站管理公司提出共享数据的请求,该公司下辖多个实体用户。运维公司主要是指根据业务需求,可以是运营商公司下辖,也可以是基站管理公司下辖,对基站的设备等进行运营维护的公司,该公司下辖实际员工的权限由实际管理公司授予,权限范围不得大于管理公司权限。

针对以上所提及的用户特点,整个动环监控系统在用户管理方面采用基于角色的访问控制模型(RBAC)来实现权限管理。RBAC 将用户模拟为角色,用户可以通过角色享有许可。该模型通过定义不同的角色、角色的继承关系、角色之间的联系以及相应的限制,动态或者静态地规范用户的行为[22]。

系统权限管理结构图 6 所示。

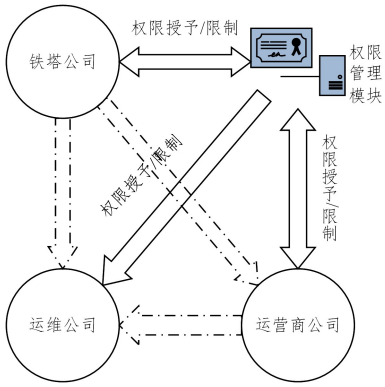

图 6　系统权限管理结构

Fig. 6　System rights management structure

如上所述，基站管理公司为动环监控系统中拥有最高权限的用户，其可对运营商公司（员工）、运维公司（员工）进行权限的授予与限制，运营商公司的管理员账号可以对下辖运维公司（员工）进行权限的授予与限制。权限授予规则的基本单位是以基站为基础的设备参数组，如表 1 所列。

表 1　设备权限参数组

Table 1　Device permission parameter group

用户组	xx 号基站访问权限	门磁传感器 1	水浸传感	温度传感器 1	门禁 1 控制权限	…
1	1	1	1	1	0	…
2	1	1	1	1	1	…
3	1	1	1	1	1	…
…	…	…	…	…	…	…

在实际系统中，可以根据业务对权限参数进行组合，以达到对基站设备权限的细粒度控制，从而使得设备的使用和数据的控制更加细致化，避免了运行数据的过度授权外露，亦使动环监控系统得到更多业务上的扩展。比如，系统可以与某一设备的运维公司共享实时数据，提高设备维护的效率和质量，而不必担心将其他数据泄露出去；另外，可以将三大运营商的设备数据进行分割，避免对以往数据的过量采集，减轻服务器的压力等。

与一般授权系统不同的是，该系统所有的授权都记录在区块链上，做到了数据的防篡改和可追溯、透明化，便于后期审计等工作的开展。

3.3.6　证书和密钥管理

上述基于区块链的动环监控系统中，所有用户与设备的参与都用到了公私钥、签名、数字证书等密码学技术，当然这也是该系统技术的基础。本节主要介绍公钥基础设施（Public Key Infrastructure，PKI）系统和系统中用户/节点公私钥、证书的分发，以及如何将其用于权限控制和通信。

对于参与本系统的实体用户，其登录系统的账户可以与区块链系统中的公钥进行绑定，以达到普通账户与区块链账户的链接，使其具有参与区块链系统的基础。

基于区块链的动环监控系统的证书管理和认证架构如图 7 所示。

1）系统中所有参与通信的 BCFSU、客户端、用户以及各类业务服务器都需要向 PKI 服务器申请通信证书。在进行申请时，需要提交相应的证明，如单位编号、个人信息等。参与区块链共识的节点的初始化是系统初始化配置或者通过管理员进行添加并分配相应的证书的。

2）当申请证书的请求到达 CA 后，CA 验证申请者的信息验证合法后向密钥管理中心（Key Management Center，KMC）提交创建申请者密钥的请求。

3）KMC 接收到请求以后，根据申请者的信息生成密钥对，并利用 DH（Diffie-Hellman）密钥交换算法将密钥发送给请求者以及 CA。请求者收到密钥对以后，以基于口令加密（Password Based Encryption，PBE）的方法对私钥进行加密存储。该方法可以使得用户在使用时再利用口令将私钥进行解密并使用。

4）另外，CA 收到 KMC 返回的关于申请者的公钥以后，根据申请者信息生成相应的证书，证书可以采用 X. 509 标准[23]。CA 将该证书返回给证书的申请者。

5）区块链参与者需要验证消息的合法性时，可以根据信息发送者的公钥或者证书信息，由系统的证书验证系统向 PKI 系统发起证书验证请求，通过查询 CRL 以及对证书的验证，验证其合法性，并返回结果。

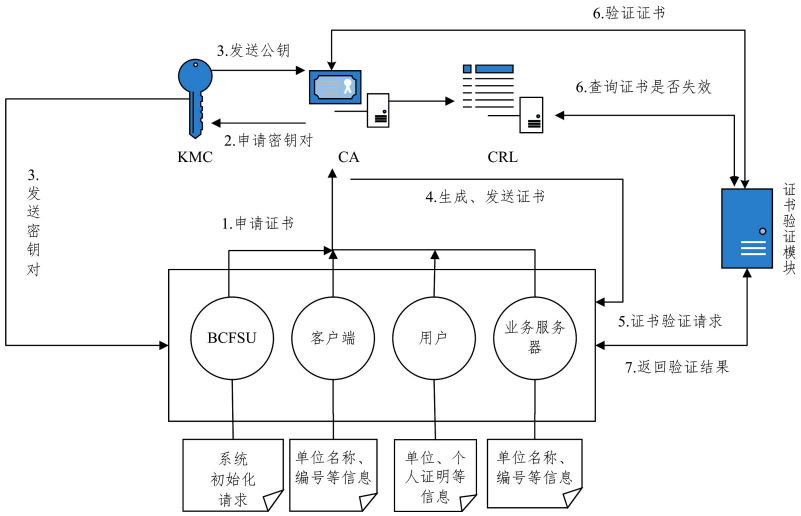

图 7　证书管理和认证架构

Fig. 7　Certificates management and authentication architecture

本区块链系统中节点间的通信信息均需要进行签名，并附带发送者的公钥，具体格式详见图 5。

此外，由于 KMC 和 PKI 等含有大量安全信息的服务器需要存放于集团公司，因此为减轻总服务器压力，可在各市基站管理公司分设副本服务器，用于处理市级请求服务，从而实现负载均衡。

3.4 交易流程模拟

为了彻底地了解基于区块链的动环监控系统的交易单的流转流程以及运行细节，本节将通过介绍一台位于 CH-000 的监控服务器 SC 向位于 CH-010 的 BCFSU0 发起门磁传感器 0 状态值的数据请求过程，来展示本系统的基本工作流程，如图 8 所示。

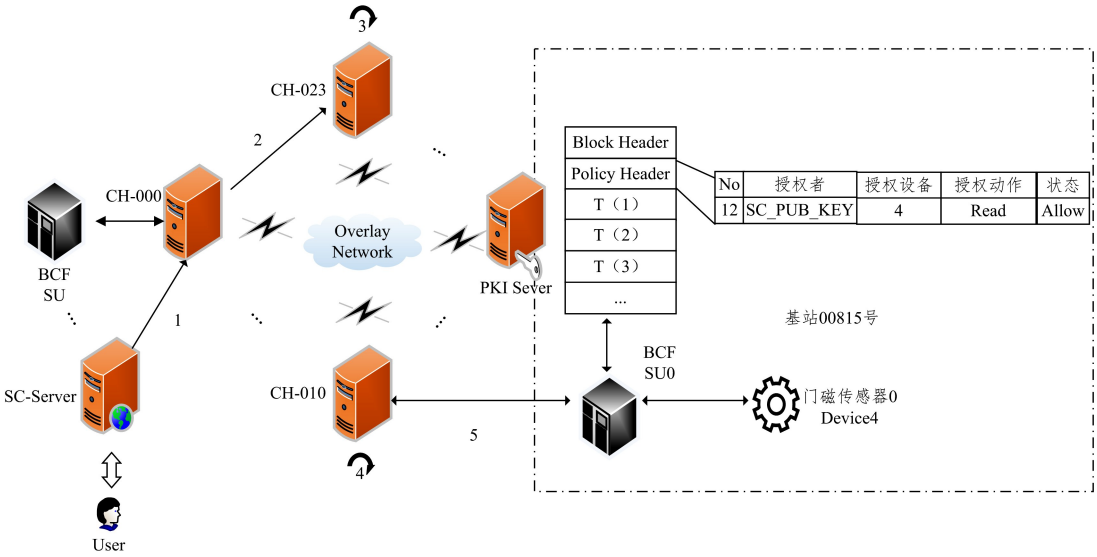

图 8 系统信息流转图

Fig. 8 System information flow diagram

1)由于业务需求，用户需请求基站 00815 号的主门的状态，即向 CH-010 的 BCFSU0 请求门磁传感器 0 的状态值。首先，SC-Server 生成请求信息 $DATA\_SC_1$，并利用 BCFSU0 的公钥对请求信息进行加密，且用自己的私钥 SC_PRI_KEY 对请求信息进行签名得到 $SIG\_DATA\_SC_1$。SC_Server 将该消息打包为区块链系统的一条交易单 Tx_SC_1，交易单信息包含加密的请求信息字段 $DATA\_SC_1$、发送者公钥 SC_PUB_KEY、服务提供者 PK(即 BCFSU0_PUB_KEY)、请求数据的数字签名信息 $SIG\_DATA\_SC_1$ 等(详见图 5)。由于该 SC-Server 接入的是以 CH-000 为 CH 节点的自治域网络(SC-Server 亦可作为轻量级节点单独接入 Overlay Network 区块链系统)，因此需要利用 CH-000 的公钥 CH-000_PUB_KEY 对该交易单信息 Tx_SC_1 进行加密，且利用自己的私钥 SC_PRI_KEY 进行签名，得到 $SIG\_Tx\_SC_1$。将消息打包完毕后发送给 CH-000 节点。

在系统中，节点间的通信信息都需要进行签名和加密，以此来确保系统中信息的机密性、完整性和有效性。后续步骤中信息的加密、签名等过程将不再赘述。

2)CH-000 收到来自 SC-Server 的信息后，查找集群的节点信息列表(3.2.1 节)中该 SC-Server 的 PK(即 SC_PUB_KEY)并对该消息的 $SIG\_Tx\_SC_1$ 进行验签，不通过则将该信息丢弃，若多次收到不通过信息，则将该端口加入黑名单，拒收来自该节点的请求(以此防止非法节点的请求，防范 DoS 等攻击)。若校验通过，则利用 CH-000_PRI_KEY 对加密的 Tx_SC_1 进行解密，解密后同样对信息的签名、发送者 SC_PUB_KEY 进行检查，并利用 SC_PUB_KEY 向 PKI Server 发起证书验证请求，若不通过，则丢弃该消息，且将该 SC_PUB_KEY 从集群节点信息列表中移除；若证书验证通过，则将该交易单 Tx_SC_1 发送给区块链系统中的主节点 p，主节点依据最长链原则，选出集群服务器中最后一个共识完成的拥有最大视图编号的服务器作为主节点[21]，经 Searching，该视图下的主节点 p 为 CH-023，并将该交易单存入服务器的待确认列表。

3)CH-023 收到 Tx_SC_1 后，对信息的完整性以及发送者证书的合法性等进行校验，校验后将消息交易单进行保存。主节点将该交易单和其他交易单进行打包，生成区块，且将区块广播到 Overlay Nertwork 中的其他节点，完成改进型 PBFT 的共识两阶段。区块的生成和验证以及 PBFT 的共识阶段，详见区块的生成和验证章节(3.3.4 节)。

4)在完成改进型 PBFT 的共识两阶段后，CH-010 同样收到包含 Tx_SC_1 交易单的区块。CH-010 在进行区块验证的过程中，检查到服务提供者 BCFSU0_PUB_KEY 在自己的集群节点信息列表中，则将对该交易单进行完整性以及证书合法性验证，若验证不通过，则不理会该消息，若验证通过，则将该交易单信息发送给 BCFSU0。同时，CH-000 收到该区块后发现区块中包含 Tx_SC_1 时，则将该交易单从待确认列表中移除，并发送确认消息给 SC-Server。

5)BCFSU0 收到 Tx_SC_1 后，对该信息进行安全性校验，若校验通过，则将该交易单打包存入本地区块链，且利用 BCFSU0_PRI_KEY 对加密的 $DATA\_SC_1$ 进行解密，并对解密后的消息 $DATA\_SC_1$ 进行解析。由于 SC-Server 请求的为门磁传感器 0 的状态值，因此 BCFSU0 向本地区块链发起权

限查询请求，检查到该 SC_PUB_KEY 对 Device4（门磁传感器 0）的 Read 动作为 Allow，则 BCFSU0 从硬件端口读取门磁传感器 0 的状态值，并根据请求信息生成回复交易单 Tx_BCFSU0 发送给自治域内的 CH-010 节点，同时将该交易单存入 BCFSU0 的本地区块链中，完成此次请求回复。

Tx_BCFSU0 的信息流转过程与步骤 1）－5）类似。

上述交易单发起流程仅为本系统中的一种类型交易，其他类型的交易单流转与此类似。特殊说明：若请求的数据为视频监控信息，则 BCFSU 将视频信息进行分片，且将数据存储于本地区块链系统的存储系统中，将其哈希值放入交易单中，视频信息则通过 FTP 等协议进行传输。另外，对于 BCFSU 的固件信息、授权信息等类型信息的更新，亦可通过该系统进行分发。由于区块链系统提供安全的分布式中心节点，将固件信息广播到 Overlay Network 中后，各节点判断交易单的类型，将交易单分发到各 BCFSU 中，由 BCFSU 判断具体需要更新的固件类型以及各项配置信息。本文提出的架构，即可减轻中心模式下固件分发中心服务器的压力，又可提供安全、高效的更新效果。

4　系统架构评估

本节将对基于区块链的动环监控系统的安全性进行分析，并将其与现有传统动环监控系统架构进行对比，以分析在动环监控系统中采用区块链技术的优势。

对于信息系统的安全性，从两方面进行分析：1）信息传输过程中的机密性、完整性和有效性；2）信息系统所面临的常见网络攻击。

本文所提出的架构以区块链技术以及 PKI 等密码学技术作为系统的基础设施，使得通信信息的加密传输在本系统中成为可能。在通信过程中对信息的加密和签名，以及对传输数据的 Hash 计算，确保了只有通信双方才能得知加密信息的真实内容，且签名技术也保障了数据的不可抵赖性，因此动环监控系统数据的真实性得到了保障。另外，由于交易单信息都是经过通信双方公钥加密，CH 节点并不保存通信双方私钥等信息，因此对于失效 CH 节点而言，其数据仅有通信相关方的信息索引，并不会泄露任何业务的相关数据信息。

在防范网络攻击层面，假设攻击者可以通过某些手段控制 BCFSU 节点、CH 节点或者其他接入系统的功能性服务器，并发起攻击。以以下几种常见的网络攻击为例，对系统的安全性进行分析。

1）拒绝服务攻击：攻击者的目标是通过大量分非法请求，导致某一服务器瘫痪而无法提供正常的服务。本文所述架构在业务上没有真正意义的中心服务器（此架构为多中心模式），该架构模式本就可以抵御常见的 DoS 攻击。即使在最糟糕的情况下，假如攻击者向某一 CH 节点发送非法请求，此时 CH 节点会通过发送者的 Pk 查找集群节点信息列表，对发来的信息进行校验，只有事先注册的合法请求才可被 CH 服务器接受。另外，CH 服务器在接收到大量不合法请求时，可以拒绝对该发送者做出响应。

2）丢弃服务攻击（Dropping Attack）：攻击者控制了作为 CH 节点的 BCFSU，拒绝对该集群中其他 BCFSU 进行信息的转发。然而，此种攻击可以被检查到，BCFSU 若在发出请求后很长一段时间没有收到关于该消息的回复信息，或者很长时间没有收到所在 CH 的消息，则会在业务既定集群内重新选举 CH，恢复通信。

3）区块打包攻击（Mining Attack）：攻击者控制了作为主节点的 CH 节点，且控制 CH 节点拒绝对区块进行打包或者拒绝接收来自其他节点的交易单。在此种情况下，节点长时间没有收到来自主节点的信息，则会认为主节点失效，从而自动更换主节点[19]，重新启动共识阶段。若某一节点更改交易单，从中作乱，则会在 PBFT 共识阶段被发现，不会达成共识。

在系统权限的安全保护上，主要通过人为干预和系统安全模块来实现。在人为干预方面，系统证书发放时的中心化，使得可以通过严格筛选系统的管理人员，设置完整的管理规章以及对参与系统的各级管理人员的权限进行明确的限定，严格审查接入材料，及时对退出系统的公司（用户）的证书进行吊销等措施，来保障系统的安全性。在系统安全模块方面，利用 PKI 系统的证书认证功能来实现对证书的有效性审查。在 BCFSU 数据获取的权限控制方面，系统在证书审查的基础上通过本地区块链的 Policy Header 中记录的权限设备参数组（见表 1）来实现用户对基站设备权限的细粒度控制。

综上所述，表 2 列出了本文所述架构在各层次所使用的安全措施。

表 2　系统各层次所使用的安全措施

Table 2　Security measures used at all levels of system

特性	BCFSU	Overlay Network
身份确认	签名、公钥	签名、证书
权限控制	Policy Header	集群节点信息列表
协议和网络安全	加密	加密
不可抵赖性	加密、签名	加密、签名
授权	Policy Header	证书、集群节点信息列表
节点抗容错	—	高

将本架构与现阶段采用的以中兴 E_Guard[7] 为代表的传统动环基站监控系统[1,4-6,8] 进行对比，结果如表 3 所列。

表 3　本系统与现有架构的对比

Table 3　Comparison of this system with existing architecture

系统	节点容错	服务器中心数量	抗 DoS 攻击	细粒度权限控制	用户管理	扩展性	数据冗余	信息加密完备程度
本文架构	有	多中心	是	是	证书	强	多	多
E_Guard 传统架构	无	1	否	否	ID	弱	少	少

可以看出，与传统架构的动环监控系统相比，本文提出的区块链系统表现出了不少优越性。其主要表现在采用多中心的区块链架构以后在分布式架构方面具有很多优点，比如抗 DoS 攻击、多中心下系统服务能力的提升、系统的扩展性的增强、服务节点容错能力的提高等都增强了系统运行的稳定性和扩展性。

另外，在采用区块链架构的基础上，充分地利用 PKI 等密码学技术，使得信息系统的安全性，以及用户和权限管理的完备性，相较于传统系统架构得到了大幅度的提升。

但是,区块链系统多中心的特点,必将会使得数据大量冗余。此外,由于 BCFSU 在动环监控系统中会被作为 CH 节点使用,这也必将提高 BCFSU 对数据处理的要求。

结束语 目前,区块链技术越来越受学术界和产业界的青睐,虽然其技术还处于前期的研究论证阶段,但是在研究者的共同努力下,其技术也越来越成熟,尤其是在 5G 基础设日渐完善,物联网应用时代来临的大背景下,物联网设备的安全性以及架构成为了发展的重点。区块链技术的特点,使得其在物联网中的应用也逐步成为一个主要的发展方向。本文初次提出基于双区块链的动环监控系统架构,为动环监控系统指明了新的发展方向,也为区块链的广泛应用提供了更多可能。尤其是将改进型 PBFT 共识协议应用于该系统,可以使系统在保障安全的前提下,以极少的算力维持系统的稳定性,同时亦可以在较少的节点环境下运行且维持其良好的扩展性,为系统前期的小规模应用和试运行提供了可能。但是,基于改进型 PBFT 的区块链系统在共识过程中仍然存在效率不高以及系统对机房内设备间基于区块链的管理还有所欠缺等情况,这也将是未来进一步深入研究的方向。

参 考 文 献

[1] CHEN G. The Software Design and Implementation of VPN Base Remote Monitoring System for Base Station[D]. Chengdu: University of Eledronic Sicence and Technology of China, 2017. (in Chinese)
陈刚. 基于 VPN 的基站远程监控系统软件设计与实现[D]. 成都:电子科技大学,2017.

[2] LUO C. ZTE E-Guard: Forerunner of security industry[J]. China Public Security, 2013(19): 93-94. (in Chinese)
罗超. 中兴力维:安防行业化的先行者[J]. 中国公共安全,2013(19):93-94.

[3] YAN B Y, WANG L G, LI H. Application and technology innovation of China tower moving ring monitoring system [J]. China New Telecommunications, 2018, 20(12): 142-143. (in Chinese)
闫佰义,王联冠,李洪. 中国铁塔动环监控系统的应用及技术创新[J]. 中国新通信,2018,20(12):142-143.

[4] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system [M]. Consulted, 2008: 24-26.

[5] DONET J A D, PÉREZ-SOLA C, HERRERA-JOANCOMARTÍ J. The bitcoin P2P network[C]// International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2014: 87-102.

[6] STALLINGS W. Cryptography and network security: principles and practice[M]. Upper Saddle River, NJ: Pearson, 2017: 743.

[7] MATTILA J. The blockchain phenomenon-the disruptive potential of distributed consensus architectures[R]. ETLA Working Papers, 2016.

[8] PETERS G W, PANAYI E. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money[C]// Banking Beyond Banks and Money. Cham: Springer, 2016: 239-278.

[9] CHRISTIAN D, SEIDEL J, WATTENHOFER R. Bitcoin meets strong consistency[C]// Proceedings of the 17th International Conference on Distributed Computing and Networking. ACM, 2016.

[10] EVANS D. Economic aspects of bitcoin and other decentralized public-ledger currency platforms[OL]. http://www.law.uchicago.edu/Lawecon/index.html.

[11] WOOD G. Ethereum: A secure decentralised generalised transaction ledger[J]. Ethereum Project Yellow Paper, 2014(151): 1-32.

[12] FABRIC-HYPERLEDGER H, HYPERLEDGER W G[OL]. https://www.hyperledger.org/projects/fabric.

[13] RIVEST R. The MD5 message-digest algorithm[R]. 1992.

[14] EASTLAKE D, HANSEN T. US secure hash algorithms [OL]. https://www.rfceditor.org/rfc/pdfrfc/rfc4634.txt.pdf.

[15] RIVEST R L, SHAMIR A, ADLEMAN L M. A method for obtaining digital signatures and public-key crypto systems[J]. Communications of the ACM, 1983, 26(1): 96-99.

[16] JOHNSON D, MENEZES A, VANSTONE S. The elliptic curve digital signature algorithm[J]. International Journal of Information Security, 2001, 1(1): 36-63.

[17] KRAVITZ D W. Digital signature algorithm[M]. Washingto, USA: World Heritage Encyclopedia, 1993.

[18] CASTRO M, LISKOV B. Practical Byzantine fault tolerance [C]// Proceedings of the Third Symposium on Operating Systems Design and Implementation. 1999: 173-186.

[19] DORRI A, KANHERE S S, JURDAK R, et al. Blockchain for IoT security and privacy: The case study of a smart home[C]// 2017 IEEE International Conference on Pervasive Computing and Communications Workshops. IEEE, 2017.

[20] EASTLAKE D, HANSEN T. US secure hash algorithms (SHA and HMAC-SHA) [OL]. https://www.rfceditor.org/rfc/pdfrfc/rfc4634.txt.pdf.

[21] GAN J, LI Q, CHEN Z, et al. Improvement research of Blockchain Practical Byzantine FaultTolerance Consensus Algorithm [J]. Journal of Computer Applications, 2019(9): 1-10.
甘俊,李强,陈子豪,等. 区块链实用拜占庭容错共识算法的改进研究[J]. 计算机应用,2019(9):1-10.

[22] SANDHU, RAVI S. Role-based access control[J]. Advances in Computers, 1998, 46: 237-286.

[23] MYERS M, ANKNEY R, MALPANI A, et al. X. 509 Internet public key infrastructure online certificate status protocol-OCSP: RFC 6960[R]. 1999.