doi:10.3772/j.issn.1002-0470.2019.10.002

基于 Fabric 架构的区块链机房管理系统设计①

胡春瀛②* 姬庆庆③** *** 肖创柏****

(*北京工业大学艺术设计学院 北京 100124)

(**中国科学院大学 北京 100049)

(***中国科学院计算技术研究所前瞻研究实验室 北京 100190)

(****北京工业大学信息学部 北京 100124)

摘 要 近年来高校不断强化信息化建设,现阶段中心化的机房管理系统极易因为各类安全问题导致无法正常使用。针对上述问题,文章结合高校网络实际环境与机房管理具体需求,设计开发了基于区块链架构的机房管理系统。该系统利用基于 Fabric 架构的区块链技术,使用非对称加密算法、拜占庭算法等技术设计开发具有安全性、可靠性及去中心化特点的机房管理系统。通过实际应用表明,该系统能够在高校局域网环境下对机房设备进行统一管理,并可面向用户开展预约服务,有效提高了机房管理效率,可满足实际应用需求。

关键词 区块链; 机房管理; Fabric 架构; 拜占庭算法

0 引 言

近些年,随着数字货币的发展,区块链(block chain)技术成为学术界重点关心和研究的领域之一。区块链技术以去中心化、分布式共识、非对称密钥加密、时间戳为核心价值[1]。这一技术为解决中心化系统普遍存在的高成本、可靠性差等问题提供了很好的解决方案。对于区块链而言,其具体的定义可以做如下描述:区块链是按照时间顺序把数据区块用与链表相似的方式构建的数据结构,以分布式共识和哈希加密的方法保证区块链数据的一致、不可篡改和不可伪造的分布式去中心化账本。可以安全存储简单的、有时间关系的、便于进行验证的数据[2],这些数据被所有节点通过分布式一致协议进行共享[3]。区块链技术的出现在很大程度上为双重支付和拜占庭问题提供了很好的解决方案[4-6],也使得这一技术成为取代传统的中心化系统的热门方案。

针对区块链应用系统的研究中,国外最有代表性的是 R3 联盟,这是由全球的几大银行联合建立的区块链联盟组织。R3 联盟针对区块链的应用开展了深入研究,主要是通过区块链去中心化的技术满足不同行业的服务需求,还开发了分布式私人区块链账本[7]。在国内,徐玉勤等人[8]研究了高效查询的高性能教育证书区块链,并通过相关实验验证区块链技术可以用于教育证书管理。

各高校均配置了面向学生开放的计算机实验中心,以满足学生课程实践与课外创新的需求。随着信息化智能化的发展,机房的管理系统也从人工管理进入到自动化智能管理。目前的机房管理系统基本是采用服务器/客户端的集中式网络管理,这种集中管理对服务器和网络安全的要求较高,一旦这个系统出现故障,如数据故障、系统平台故障、监管失

① 国家自然科学基金(61501008),北京市科技计划(Z171100004717001)和北京市自然科学基金(4162007)资助项目。

② 女,1974 年生,硕士,实验师;研究方向:区块链技术,网络安全,大数据技术;E-mail: huchunying@bjut.edu.cn

③ 通信作者,E-mail: 1602584488@qq.com

(收稿日期:2019-01-19)

灵、人为入侵等问题,就会严重影响实验中心的开放使用。目前对于机房管理系统的研究大多围绕物联网技术、虚拟现实技术等展开,这些改进很难从根本上解决机房管理系统所面临的安全问题[9]。本文将区块链技术引入机房管理系统的开发构建,相比传统机房管理系统,它不仅能够保障系统的自动化运行,还使这个系统更加安全可靠,数据不可篡改,并且对于使用者、管理者、监督者等信息的透明度都有所提升[10]。

本文在充分了解高校机房管理的业务流程和实际需求的基础上,设计并开发了一种基于 Fabric 架构的区块链机房管理系统。利用该系统可以满足高校对机房进行去中心化管理,提高管理效率;同时还能够利用区块链技术的特点保障用户信息不被他人窃取。系统结合校园机房管理实际需求,创新性地结合校园局域网开发区块链机房管理系统,相较于常见区块链应用系统基于云存储、云服务的模式具有更高的安全性[11,12]。

1 区块链机房管理系统构建

基于校园网环境的机房往往用于服务在校师生,一方面为教务处开设的计算机相关课程提供配套的上机实践环节;另一方面为师生利用课余时间开展创新实验、参加学科竞赛等自主实践活动提供便利条件。本系统针对基于校园网环境下的机房进行开发,系统具体设计如下。

1.1 系统模型

基于区块链技术的机房管理系统模型如图 1 所示。系统共涉及学生、教师、管理员、财务 4 个模块,和预约、上下线、管理 3 个智能合约。在职教师和学生的信息会通过校园一卡通中心数据库导出并植入本系统。学生模块主要包含预约和查询功能;教师模块比学生模块增加课程预约功能;管理员模块主要是用户信息的维护、机器信息的维护和对机房及机器使用情况的查询;另外还有财务模块,即起到运行监督的作用,也可以查询本系统的收益情况。

系统运行中生成的数据信息,会通过智能合约运算存储在记录池中,系统中有多个记录池,彼此间可互通信息,这也是去中心化系统对于数据安全性的保障。为提高系统数据处理速度,要尽可能在区块链上少存储数据信息,本系统只在链上存储维持运行必要的信息[13-16]。

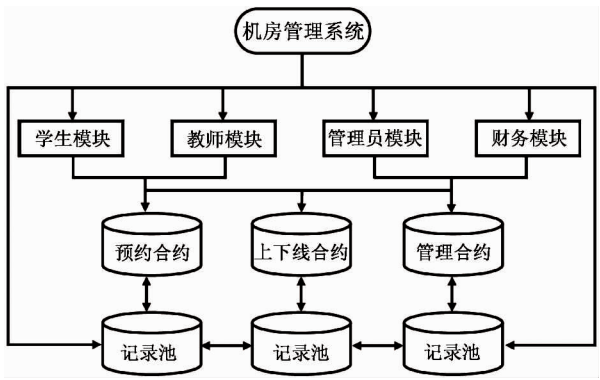

图 1 区块链机房管理系统模型

1.2 系统组成

校园机房管理系统拥有多个机房,每个机房又有数十台计算机。系统中的主体(学生、教师、管理人员、监管人员等)还可以远程使用 App 终端完成预约和查询功能。传统的中心化管理对系统安全与稳定性要求很高,也使系统的能耗较大,联盟区块链构建的新系统实现了数据的分布式安全存储[17],如图 2 所示。

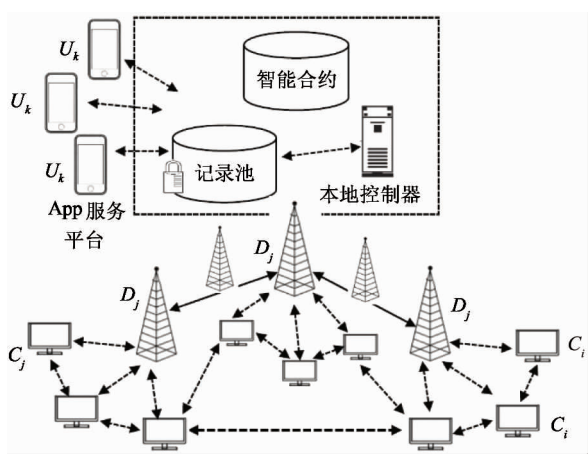

图 2 数据存储联盟链系统组成

1.2.1 节点管理

(1)计算机节点(C_i)。每个电脑终端即为 1 个节点,节点是构成区块链机房管理系统的基本元素。

(2)数据聚合器(D_j)。每个机房设有 1 台数据聚合器(数据基站),它们通过有线网络彼此链接,

不仅用以采集本机房内各节点的信息、存储全网数据区块,还有个重要任务——达成联盟区块链共识机制。数据聚合器间可以互相通信,在收集信息的过程中它们构成协调合作的整体,在寻找有效的工作量证明(proof-of-work,PoW)时它们又会彼此竞争,争取记录本次区块以获得奖励。这样即节省了节点的能耗,又加速了达成共识的时间。

(3)记录池与本地控制器。每个数据聚合器都包含有数据记录池和本地控制器。区块链上的数据存放于数据记录池。本地控制器负责感知节点上的数据,执行智能合约[18]。

(4)智能合约。智能合约是 1 个运行在去中心化的计算机网络中的程序脚本,可以依据设定的约束条件自动执行数据处理与共享等操作,并且具有过程透明、不可篡改、可追踪等特点。

(5)App 服务平台。为方便用户(U_k)使用本系统而搭建的终端预约与管理平台,App 数据通过无线网络接入机房管理区块链,并在区块链内作为基本数据信息进行共识处理与记录。

1.2.2 节点发现

在这个基于 Fabric 的区块链中,每个节点都可以自动推送信息或者收取信息,各节点的权限是不一样的。数据聚合器(D_j)是系统里的超级节点,新的数据生效必须经过数据聚合器的认定。在不影响系统运行的情况下,数据聚合器同时可以进行人工管理,更新信息。

启动系统服务功能后,首先加载各数据聚合器,获取 D_j 值,保存 1 个临时变量在计算机节点(C_i)上;然后 C_i 将自身数据与前面链接信息整合加密,生成请求信息,推送到网内;数据聚合器获取到 C_i 返回的信息后更新数据记录。

本研究所使用的主要符号代码的含义如表 1 所示。

表 1 文中所用符号含义表

	含义	备注
C_i	第 i 个计算机节点	*Computer*
$Data_j$	第 j 个数据聚合器(数据采集器)	*Data aggregator*
U_k	第 k 个用户节点	*User*
ID	主体 *ID* 编号	
$i \rightarrow j$	主体 i 发送信息给主体 j	
PK_i	主体 i 的公钥	*Public Key*
PK_i	主体 i 的私钥	*pRivate Key*
$Cert_i$	主体 i 的证书	*Certificate*
$Sign_i$	主体 i 的签名	
Data _ set	数据集合	
Hash(M)	信息 M 的哈希值	
Bits	难度系数	
Rand _ Num	随机数	
$X \parallel y$	元素 x 连接元素 y	
$E_{PK_i}(M)$	用主体 i 的公钥加密信息 M	*Encryption*
$Sig_{RK_i}(M)$	用主体 i 的私钥对信息 M 进行数字签名	*Signature*
TimeStamp	时间戳	
Record	上传的数据	

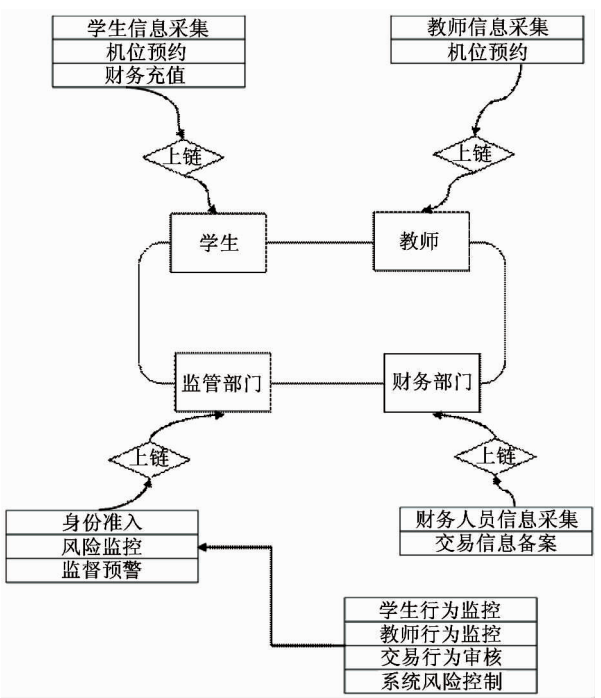

图 3 机房管理系统整体流程图

2 区块链机房管理系统功能实现

2.1 业务流程

机房管理系统整体流程图如图 3 所示,系统主要涉及预约和查询等环节,但由于参与者由学生、教师、财务人员及监管人员构成,因此各个模块之间需要高效协同,从而保障系统准确运行。应用区块链

技术的机房管理系统主要包含 4 个核心节点:学生节点、教师节点、财务部门节点和监管部门节点。下面将结合具体模块对数据提交和数据查询流程分别进行说明。

2.1.1　数据提交流程

以用户预约机时为例,数据提交流程如图 4 所示。预约开始,系统调用软件开发工具包(software development kit,SDK),包括主体 ID、数据包、个人私钥;SDK 会调取数据提交方法,依据主体 ID,到区块链节点上查询主体的公钥;如果公钥与主体 ID 不匹配,程序返回要求主体重新提交个人信息;如果公钥与主体 ID 匹配,则用主体的私钥加密数据并签名;接下来进入财务审核,如果主体账户的余额不足,则提示余额不足,程序直接结束;如果主体账户里的余额可以支付本次预约,则交易达成;SDK 调用区块链接口,并且提交数据给区块链节点,节点依据相关合约进行数据记录;预约成功,整个流程结束。

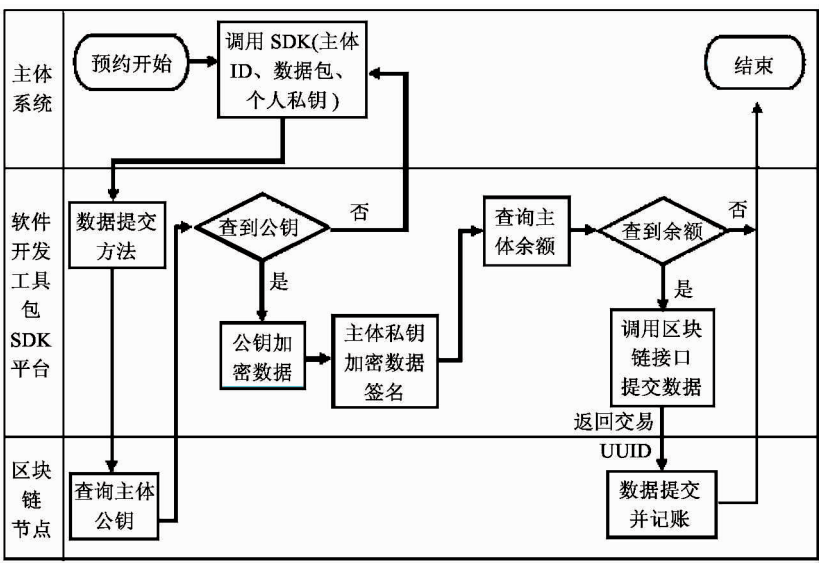

图 4　提交数据流程

2.1.2　数据查询流程

以教师或者学生用户在系统中进行查询为例,查询数据流程如图 5 所示。查询开始,系统调用软件开发工具包SDK(包括主体ID、查询请求、个人

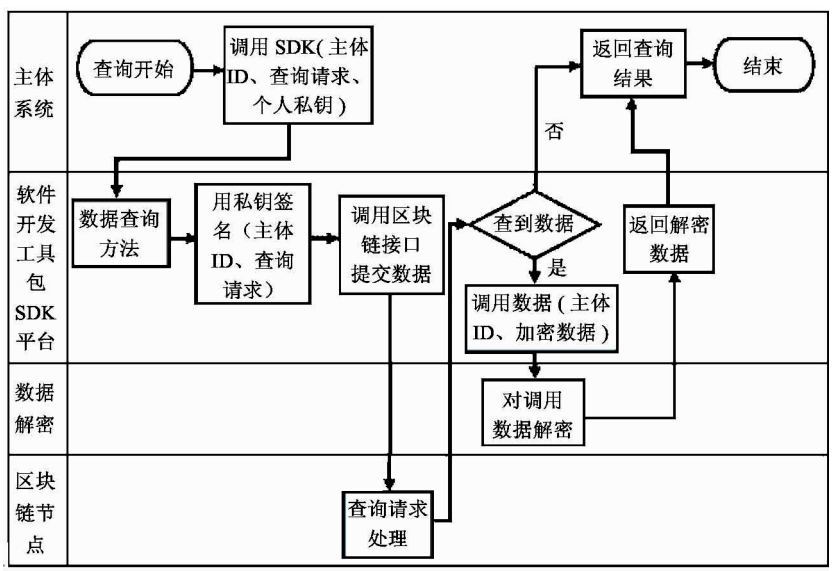

图 5　查询数据流程

私钥);SDK 会调取数据查询方法,用主体私钥对主体 ID 和查询请求信息进行签名,进而调用区块链接口并提交数据查询请求;区块链节点对查询请求进行身份验证,验证成功后提取查询的数据信息;如果没查到所需信息,提示查询结果,程序结束;如果查到所需信息,这个信息此时是加密状态,还需要发去数据解密中心进行解密,然后返回解密数据给用户主体,查询结束。

2.2 安全校核

基于区块链的系统是一个自主运行的系统,安全功能的实现尤为重要,安全校核就是对无约束交易计划进行的网络安全约束校核[19]。具体在机房管理系统中就是对公钥和私钥的管理和实现。

2.2.1 密钥生成

系统中的使用者信息均来自校园网统一用户数据库,主体私钥由系统管理者进行初始设置,使用者可登录信息系统重置主体私钥,私钥一旦修改,便会加上主体加密签名,其他主体,包括管理员和监管人员都无法获取。数据公钥则是在数据产生时设置的密钥,存在全网链中,登录可查,任何用户都可以用自己的公钥加密一段数据。

2.2.2 密钥核验

安全校核的核心是主体公钥和主体私钥非对称双重加密技术,双重加密确保了数据的安全和可靠。本研究以预约机时的操作为例进行分析,加密数据的过程可参考图 3 中流程。

软件开发工具包 SDK 依据算法到区块链节点上查询主体公钥 PK_i,如果没查到会默认输入有误,返回上一级重新提供主体相关信息并再次调用 SDK;如果查到主体公钥,SDK 会用此公钥加密提交的数据,表示为 $E_{PK_i}(M)$。SDK 使用主体私钥对主体 ID、公钥加密数据包进行签名,表示为 $Sig_{RK_i}(ID \parallel M)$。返回信息后更新数据记录。

2.3 财务审核

2.3.1 奖惩机制

系统里的币池初始化时将投放 10 000 枚虚拟货币,待系统运行起来可以实际现金转换虚拟货币,1 元人民币 = 100 单位虚拟货币。因使用本系统为主体硬性需求,所以采用的是低奖励高惩罚的方式,以保证币池里的虚拟货币不会用光。惩罚主要目的是维持这个自运行系统的秩序。例如,如果用户超过预约时限不下线,在本自动运行的系统里没有任何强制下线的机制,只能依靠高惩罚制度维护用户的自觉性,会进行 10 倍于单位时长的收费金额,加大违约成本。如果用户账户里余额不足以支付罚金,则会以负金额计入该用户账户,用户如果不充值,会影响以后使用,如以后不再使用,在其离校清理财务账户时由学校财务系统处理。

用户使用本系统产生的使用费和罚金,由学校统一安排处理,可主要用于补充系统维护资金。

2.3.2 余额核准

本系统在记录数据前还要对主体的财务账户进行余额核准。财务系统作为监管机构接入联盟区块链中,当主体预约信息生成后,SDK 会调用校园财务系统,查询其余额是否足以支付本次使用,如果余额不足,进行提示后预约程序直接结束,主体需要去账务提供的充值平台进行充值,本系统不提供充值服务。余额合格设置:以每小时 1 元使用费为例,其账户余额 =“其计划预约时长”×“1”元。如果余额充足,SDK 才会调用区块链接口提交数据。

2.4 记录数据

2.4.1 工作量证明机制

数据聚合器(基站)会收集本地所有节点的数据信息,并进行签名校验,如果成功则将记录信息存入记录池,如校验不成功直接丢弃数据。聚合器还要每隔一段时间(一般为 10 min)收集链上所有数据聚合器的有效数据记录,并进行数据整合,具体表示如下:

$$Data\_set = \{block\_head \parallel block\_body \parallel timestamp\}$$

每个数据区块一般包含区块头和区块体 2 部分。区块头主要包括版本号 *version*,前一区块地址 *PrevBlock*,时间戳 *timestamp*,随机数 *Rand_Num*,当前区块的目标哈希值即难度 Bits,Merkle 树的根值 *hashMerkleRoot* 等信息,计为 *block_head*[20,21]。区块体记录了一段时间的所有交易信息,主要包含交易的计数和交易账单详情,计为 *block_body*。区块头大小为 80 字节,结构格式化,区块体数据信息则比较大,最终会运用哈希算法对区块体中的数据进

行计算,得到 1 个 Merkle 树根值存于区块头中[22]。

寻找工作量证明,其具体过程是数据聚合器通过随机数 *Rand _ Num* 和上一个区块的区块头(PrevBlock)数值来计算当前区块的哈希值的过程。也即计算满足 $\{Hash(Rand\_Num + PrevBlock) < Bits\}$ 的随机数 *Rand _ Num*。这里 *Bits* 是系统用于约束数据集合器计算出正确的随机数 *Rand _ Num* 的速度,该值会依据系统实际计算能力不断调整,以维持 10 min 产生 1 个数据块的频率。最先计算出正确 *Rand _ Num* 值的数据聚合器将全网广播当前数据集合和计算出来的 *Rand _ Num* 值(即工作量证明 PoW),如果其他数据聚合器也认可该 *Rand _ Num* 值对应的工作量证明,该数据聚合器就会将数据集合整合成新的数据区块,并存储在联盟链上,同时获得相应的系统奖励。在这个新区块数据的基础上,将会开展后续工作量证明的计算。

2.4.2 拜占庭容错算法

拜占庭容错算法(practical Byzantine fault tolerance,PBFT)也是一种常见的共识证明[23]。它以计算为基础,也不存在代币奖机制,由区块链上所有用户参与投票,当 $(N-1)/3$ 个节点数以下反对时就拥有公示信息的权利[24]。机房管理系统即采用这种投票机制。最快计算出有效工作量证明的数据聚合器 ($Data_j$) 成为主节点,它将自己整合的数据区块加上哈希值和数字签名后,向链上所有节点进行广播,以期被其他节点审核通过,通过即为投上 1 票。

具体表示如下:

$$Data_j \rightarrow All: Record = (Data\_sets \| Data\_hash \| Cert_{Data_j} \| Sig_{Data_j} \| Cert_{U_k} \| Sig_{U_k} \| timestamp)$$

其中:

$$Data\_hash = Hash(Data\_sets \| timestamp)$$

$$Sig_{Data_j} = Sign_{RK_{Data_j}}$$

$$Sig_{U_k} = Sign_{RK_{U_k}}$$

其他节点称为从节点,每个从节点都会完成 2 项任务,当接收到主节点发出的数据区块及哈希值、数字签名等信息时,要对数据区块的合法性和正确性做验证,并把验证结果附上自己的数字签名再广播给链上其他的从节点,以实现从节点间的监督与互验。另一项任务是,从节点将其他节点的验证结果收集并汇总,并与其自身的验证结果开展对比工作。之后,主节点会收到每个从节点向其发送的回复(*Reply*),其中包含从节点自身的验证结果(*My _ result*)、收到的所有验证结果(*Rece _ results*)、验证比对的结论(*Comparison*)和相应的数字签名。同理,用户节点也参与到数据验证的过程中。

上述过程具体表述如下:

$$D_i \rightarrow Data_j: Reply = E_{PK_{Data_j}}(Data\_3 \| Cert_{Data_i} \| Sig_{Data_j} \| timestamp)$$

$$U_i \rightarrow U_k: Reply = E_{PK_{U_k}}(Data\_3 \| Cert_{U_i} \| Sig_{U_i} \| timestamp)$$

其中:

$$Data\_3 = (my\_result \| Rece\_results \| Comparison)$$

$$Sig_{Data_j} = Sign_{RK_{Data_j}}(Data\_3)$$

$$Sig_{U_i} = Sign_{RK_{U_i}}(Data\_3)$$

来源于所有从节点的审计回复被主节点最终汇总。假设有 100 个节点,如果不赞同的验证结果少于 $(100-1)/3 = 33$ 个节点,就表示当前数据区块具有合法性和正确性。主节点再次把该数据区块发给所有从节点,这次会附上参与审计的从节点的证书集合 ($\{Cert_D\}$) 和数字签名,同时该数据区块会以时间先后的顺序存储在区块链中。

上述过程具体表述如下:

$$Data_j \rightarrow All: Data\_block (Data\_5 \| Sig_{Data_j} \| timestamp)$$

$$U_k \rightarrow All: Data\_block (Data\_5 \| Sig_{U_k} \| timestamp)$$

其中:

$$Data\_5 = (Data\_sets \| Data\_hash \| \{Cert_D\} \| \{Cert_U\} \| timestamp)$$

$$Sig_{Data_j} = Sign_{RK_{Data_j}}(Data\_5)$$

$$Sig_{U_k} = Sign_{RK_{U_k}}(Data\_5)$$

另一种情况,如果有大于等于 33 个从节点不赞同验证结果,主节点将分析和查验这些数据聚合器的审计结果。判断这些数据聚合器是否有恶意行为,及时对恶意数据聚合器进行分析。此步骤对于及时发现并剔除非法恶意数据聚合器,保证系统的

安全稳定运行具有重要意义。必要时,这部分数据聚合器接收由主节点发送的该区块数据进行二次审计,如果不赞同的节点仍不满足“少于 $(N-1)/3$ 个节点”的条件,此数据区块将不被系统记录。

3 性能指标测试

为了验证区块链机房管理系统的实用性,本文结合机房实际情况模拟了一个测试环境,并在该环境下对系统开展应用验证,检验不同功能模块的运行状况。

上述测试环境中,硬件部分包括 65 台计算机及 1 台服务器,服务器具有 8 核处理器,16 G 内存。其中有 63 台计算机被均分为 3 组,模拟 3 个机房环境,每组存在 1 台计算机为教师机,还有 1 台计算机模拟管理员身份,其余 1 台计算机模拟财务管理员身份。上述所有设备间都使用以太网进行连接,所有的设备和计算机都通过交换机连接到校园局域网下,即在真实使用场景下对本文系统开展实际验证。

实验过程如下:

(1)启动系统服务器,将各个计算机节点连入所搭建的局域网环境。启动区块链网络,将各计算机节点信息录入机房管理系统。通过管理员所在计算机授予教师计算机、财务计算机及普通计算机相应权限。在服务器中建立使用人信息,将使用人引入管理系统,使之成为链上节点,同时赋予该使用人预约权限。完成上述步骤,意味着机房管理系统成功启动。

(2)通过使用人信息利用 App 登入系统开展预约工作,选取机房中任一计算机进行预约。预约结束后,管理员可以查看到预约信息,其他用户可以在 App 中利用公钥查看该条预约信息,被预约的计算机及机房其他计算机亦收到该条预约信息,被预约计算机所在机房教师机接收到该条预约信息。

(3)通过使用人信息利用 App 登入系统进行支付,财务计算机节点显示预约信息及支付信息。

系统的性能测试指标如表 2 所示。

表 2 性能测试指标

性能	指标
每条预约处理时间	1 200 ~ 1 400 ms
吞吐量	800 ~ 900 条/s
每秒处理预约数	400 ~ 420 条
数据传输准确率	99.9%
加密成功率	100%
预约成功率	99.5%

从实验中可以看出,每条预约成功处理的时间在 2 s 以内,完全能够满足校园机房日常管理的需求。实验中数据传输准确率达到 99.9%,经过分析,认为产生误差的原因是网络的不稳定。在实际网络场景中,网络环境会受到各种因素的干扰,数据传输不可避免地会存在一定程度上的损失。通过实验验证加密算法对于数据的加密过程可靠性极高,在测试过程中取得了 100% 的加密成功率。受到网络稳定性等因素的影响,测试过程中取得了 99.5% 的预约准确率,能够满足校园机房管理需要。受服务器性能、节点数及 Fabric 架构本身因素的限制,测试环境下每秒能够完成约 400 条预约请求。

传统的机房管理流程如图 6 所示,往往需要教师/学生提出申请,并在登记簿上进行登记。然后由机房管理人员决定是否通过该申请,若申请通过,机房管理人员通过机房管理系统对使用者进行授权,使用者方可使用。这种模式机房预约流程复杂,对于预约请求的处理效率低下;由于整个机房受机房管理人员所使用的计算机控制,极易引发安全状况波及整个机房从而造成机房无法正常使用的情况,继而带来严重的后果。综上而言,高度中心化的机房管理系统不仅会由于预约流程繁琐导致使用效率低下,还存在着无法忽视的完全问题,而去中心化的机房管理系统则能够有效避免这些问题。

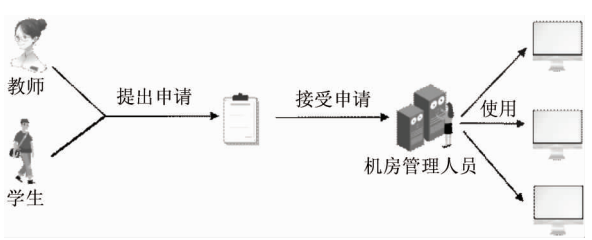

图 6 传统机房管理流程图

结合实验结果可以发现,区块链机房管理系统与传统机房管理系统相比,具有以下优势:

(1)系统安全稳定

传统管理系统是将数据以明文的形式集中存储于中心服务器上,同时将服务器中的数据复制到备份数据库中,但这种数据存储抵抗网络病毒的能力较弱,数据的容错能力较差。本文系统数据存储于全网的数据聚合器上,并实时更新,且区块链的数据区块存储方式很大程度上提升了数据的容错性也使用户数据的安全性得到提升。系统采用的非对称加密技术对数据具有 100% 的加密成功率,使得系统被网络病毒攻击的可能性大大下降,只要不是全网所有参与的节点同时故障或者崩溃,这个系统的数据存储就一直有效可读[25]。校园局域网安全一直以来都是各个高校网络安全重点关注的领域,本系统为防止校外人员开展恶意攻击,具有创新性地在校园网环境下搭建区块链架构并开发相应的管理系统。相较于现阶段常见的区块链系统利用云服务搭载区块链架构,虽然会损耗一定的数据吞吐量,但能够最大限度保障校园机房安全及校园网网络安全。

(2)数据公开可靠

传统管理系统很多数据只有管理员及监管部门可以查看,但数据的真实性难以考证,例如管理员可以修改数据记录。在本文系统中,一切数据信息都真实可靠,每条记录信息都通过节点的密钥加密后才上传数据聚合器,除非有攻击者窃取了节点的全部密钥,进而获取完整数据。另一方面,每条数据信息存入数据聚合器前盖上了时间戳,攻击者即使窃取部分数据,也无法篡改数据。对于系统的各主体,网络数据公开透明,不可篡改且全网可查,方便用户查看各节点信息,也方便监管部门掌握机器使用率等情况。

(3)运行成本降低

传统的机房管理系统采用的是中心化的管理方式,依托服务器/客户端的传统模式,为保障系统的稳定运行,对服务器等系统硬件的要求较高,对硬件的维护成本也较高,同时传统系统的运行还需要投入相当的人力成本。本文系统采用分布式结构,充分利用了网络中的各节点进行数据存储,不再只依靠服务器,降低了硬件需求成本。同时,基于区块链的机房管理系统是一个依靠智能合约构建的自主运行系统,具有高度的自治性,除了各个参与节点以外,能够最大限度减少人员干预,有效节约了人力成本。

4 结 论

本系统使用去中心化的 Fabric 架构设计了基于区块链的校园机房管理系统,利用拜占庭容错算法、工作量证明机制等区块链技术实现机房系统自动运行和数据信息的自动管理。系统开发过程中根据实际需求,将高校机房的管理者、使用者及设备纳入区块链节点,并在校园网环境下进行组网运行,保证系统的安全性。相比传统的依靠中心服务器存储数据的机房管理自动化管理方法,本管理系统不仅具有高度自治、分布式对等、去中心化、可溯源、集体维护和无法篡改等区块链技术的共性优点,还具有系统安全稳定、数据公开可靠、运行成本降低的特点。该系统在本校某机房已经开展过多次实验验证,在教师预约场景下已经开始实际应用。系统留有合理的开发接口,在未来可以根据实际需求引入更多功能模块,同时可以引入更多计算机节点进入机房管理系统参与统一管理。

尽管目前系统已经进入试运行阶段,但也要指出任何技术都不是完美的。在本系统中,由于共识机制的达成取决于节点投票,当恶意攻击占领了系统 1/3 的节点,便会破坏系统的运行,且因为没有 Token 金额的约束,犯罪成本低下。此外,本系统的单位时间交易量受限并且数据生效有延时,每次预约的信息都不会及时生成,系统中节点达成共识需要一定时间,达成共识后预约才能生效。解决这些问题还有待进一步深入研究。

参考文献

[1] 于雷, 赵晓芳, 金岩, 等. CHB-Consensus:一种基于一致性哈希算法的区块链共识机制研究[J]. 高技术通讯, 2018,28(9-10):771-783

[2] 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

[3] Karger D, Lehman E, Leighton T, et al. Consistent hashing and random trees: distributed caching protocols for relieving hot spots on the world wide web[C]//Proceedings of the 29th ACM Symposium on Theory of Computing, EI Paso, USA, 1997: 654-663

[4] Fan J, Yi L T, Shu J W. Research on the technologies of Byzan-tine system[J]. *Journal of Software*, 2013, 24(6):1346-1360

[5] Lamport L. The weak byzantinegenerals problem[J]. *Journal of the ACM (JACM)*, 1983, 30(3):668-676

[6] REISCHUK R. A new solution for the Byzantine generals problem[J]. *Decision Support Systems*, 1985, 1(2):182

[7] Brown R G, Carlyle J, Grigg I, et al. Corda: an introduction[EB/OL]. https://static1.squarespace.com:R3 CEV, August, 2016

[8] Xu Y, Zhao S, Kong L, et al. ECBC: a high performance educational certificate blockchain with efficient query [J]. *International Colloquium on Theoretical Aspects of Computing*, 2017,10580: 288-304

[9] 戴震军. 农林院校机房管理系统设计模式研究与实现[D]. 长沙:中南林业科技大学计算机与信息工程学院, 2017: 18-24

[10] Kim H W, Jeong Y S. Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain[J]. *Human-centric Computing and Information Sciences*, 2018, 8(1):11

[11] Yang D C, Zhao X Y, Xu Z X, et al. Developing status and prospect analysis of blockchain in energy internet [J]. *Proceedings of the CSEE*, 2017, 37(13):3664-3671

[12] Xing B, Marwala T. The synergy of blockchain and artificial intelligence[J]. *Social Science Electronic Publishing*, 2018, 8:1-12

[13] Lin Q, Chang P, Chen G, et al. Towards a non-2PC transaction management in distributed database systems [C]//SIGMOD Conference, San Francisco, USA, 2016: 1659-1674

[14] 于雷, 金岩. 区块链全局账本数据的拆分技术研究[J]. 高技术通讯,2017,27(11-12):875-888

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

[16] Malone D, O'Dwyer K J. Bitcoin mining and its energy footprint[C]//Irish Signals & Systems Conference & China-ireland International Conference on Information & Communications Technologies, Limerick, Ireland, 2014: 280-285

[17] Subramanian, Hemang. Decentralized blockchain-based electronic marketplaces[J]. *Communications of the ACM*, 2017, 61(1):78-84

[18] 吴振铨,梁宇辉,康嘉文,等. 基于联盟区块链的智能电网数据安全存储与共享系统[J]. 计算机应用, 2017,37(10):2742-2747

[19] Sharples M, Domingue J. The blockchain and kudos: a distributed system for educational record, reputation and reward[J]. *European Conference on Technology Enhanced Learning*, 2016, 9891: 490-496

[20] Douceur J R. The sybil attack[C]//The 1st International Workshop on Peer-to-Peer Systems, Berlin, Germany, 2002: 251-260

[21] Courtois N T, Grajek M, Naik R. Optimizing SHA256 in bitcoin mining[J]. *International Conference on Cryptography*, 2014, 448: 131-144

[22] Hovland G, Kucera J. Nonlinear feedback control and stability analysis of a proof-of-work blockchain[J]. *Modeling Identification & Control*, 2017, 38(4):157-168

[23] Bouchard S, Dieudonné Y, Ducourthial B. Byzantine gathering in networks[J]. *Distributed Computing*, 2016, 29(6):435-457

[24] Sivakami R, Kadhar Nawaz G M. A radical block to byzantine attacks in mobile Ad Hoc networks[J]. *Wireless Personal Communications*, 2016,87(2):485-497

[25] Bano S, Sonnino A, Al-Bassam M, et al. Consensus in the Age of Blockchains[J]. *arVix*:1711.03936, 2017: 4-6

Design for computer room management system based on BlockChain of hyperledger fabric

Hu Chunying[*], Ji Qingqing[**,***], Xiao Chuangbai[****]

([*] College of Art & Design, Beijing University of Technology, Beijing 100124)

([**] University of Chinese Academy of Sciences, Beijing 100049)

([***] Advanced Computing Research Laboratory, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190)

([****] Faculty of Information Technology, Beijing University of Technology, Beijing 100124)

Abstract

As universities continue to strengthen information construction in recent years, the management system for centralized computer center can't be working well due to various security issues. Regarding the above problems and considering the actual environment of the university network with the specific needs for the computer center, a management system is designed and developed based on the blockchain technology with the Fabric architecture and using asymmetric encryption algorithm with Byzantine algorithm, which has the security, reliability and decentralization characteristic. The on-site practice indicates that the designed system can effectively manage the relative equipment in the intranet environment and provide reservation service for users, therefore, the built management system not only completely meets the actual requirements, but also greatly improves the management efficiency for the computer center.

Key words: blockchain, management for Internet data center, hyperledger Fabric, Byzantine algorithm