

基于联盟链的建筑行业标准管理系统

姚勇锋¹, 孙恩昌¹, 张延华¹, 李萌¹, 曾涛²

(1. 北京工业大学 信息学部, 北京 100124; 2. 中建科技集团有限公司, 北京 100070)

摘要: 标准化工作对装配式建筑的持续、健康发展起着基础性、战略性和引领性的作用; 针对建筑行业标准正式发布后, 缺少信息技术支撑的标准全生命周期、高效能管理机制的问题, 文章做出了相关探索及实践, 提出并实现了一种基于联盟链的建筑行业标准管理系统设计方案, 利用联盟链高可信和智能合约去中心化的特点解决了标准更新过程中基于信任高效达成共识的问题, 结合 IPFS 分布式文件存储技术克服了区块链无法保存文件的难题, 最后利用开发的分享社区子系统与标准使用方建立过程反馈机制, 收集使用意见, 便于标准的迭代完善, 实现对标准的全生命周期管理。

关键词: 联盟链; 智能合约; IPFS; 标准全生命周期管理

Prefabricated Component Traceability System Based on RFID and Blockchain

Yao Yongfeng¹, Sun Enchang¹, Zhang Yanhua¹, Li Meng¹, Zeng Tao²

(1. Beijing University of Technology, Faculty of Information Technology, Beijing 100124, China;

2. China Construction Science & Technology Co., Ltd., Beijing 100070, China)

Abstract: Standardization plays a fundamental, strategic, and leading role in the sustainable and sound development of prefabricated buildings. Aiming at the problem of the lack of information technology-supported full-life standard and high-efficiency management mechanism after the official release of the construction industry standard, this paper has made relevant explorations and practices, and proposed and implemented a design of the construction industry standard management system based on the alliance chain. First, we use the high reliability of the alliance chain and the decentralization of smart contracts to solve the problem of reaching consensus based on trust and efficiency during the standard update process. Then, combined with the IPFS distributed file storage technology, the problem that the blockchain cannot save files was overcome. Finally, the developed sharing community subsystem and standard users are used to establish a process feedback mechanism and collect usage opinions to facilitate the iterative improvement of the standard and achieve the full life-cycle management of the standard.

Keywords: alliance chain; smart contracts; IPFS; standard full life cycle management

0 引言

装配式建筑作为一种新兴的建筑施工方法正在成为现代建筑业发展的主流方向。由于我国装配式建筑发展起步较晚, 国内的技术标准体系不健全, 标准化程度过低, 缺乏统一的装配式建筑行业标准, 导致建设过程中整体协调性不足, 企业间的配合度非常低, 阻碍了装配式建筑的发展进程^[1]。

针对这一问题, 行业主管单位、龙头企业、标准权威机构和大学等单位发挥产学研用优势, 以解决标准供给侧改革为突破口逐步推进装配式建筑的行业标准化水平。同时, 也随着新一轮科技革命和产业变革步伐, 利用新一代信息技术推进建筑行业标准化管理水平, 促进建筑行业标准的全生命周期、高效能管理。

随着标准正式发布、使用的企业不断增加, 标准也需要不断地更新, 各参编单位联合起来准备建立一个标准管理系统, 对标准文件存储、标准版本更新以及标准共识进行统一的信息化管理。但传统的标准信息管理系统都是将大量标准信息存入数据库中, 利用计算机技术和网络信息技术为相关单位及人员提供全面快速的标准管理服务, 进而提高工作效率^[2]。而标准都是权威性的重要文件, 这些中心化的标准管理系统存在标准文件易篡改的问题, 标准共识过程中也存在信任问题, 且标准建立后, 更新机制缓慢, 其完善可能跟不上实际应用的节奏, 系统需建立与标准使用方的服务通道, 提高标准小版本快速修改的效率, 促进标准的与时俱进。

以推动高质量发展标准体系为中心, 为构建新一代信息技术为基础的标准全生命周期、高效能管理做出有益的探索, 本文提出并实现了一种基于联盟链的建筑行业标准管理系统的设计方案, 该系统将每个参编单位绑定为一条联盟链, 联盟链中各节点组织可以通过 Web 端上传新版标准文件至 IPFS (inter planetary file system, 星际文件系统) 账本中, 当有标准文件上传时, 各节点需要对新版标准进

收稿日期: 2020-03-02; 修回日期: 2020-03-20。

作者简介: 姚勇锋(1995-), 男, 湖南邵阳人, 硕士生, 主要从事区块链技术方向的研究。

通讯作者: 曾涛(1972-), 男, 四川南充人, 硕士, 高级工程师, 主要从事工业化建造技术方向的研究。

行投票共识，共识达成后将投票结果和标准哈希值通过智能合约存储在区块链中，同时建立标准分享社区，将新标准发布到相应的分享社区子系统内，可供各建筑子公司使用，并发表相应意见。此外，系统还为联盟节点设立了相应的查询系统。

1 区块链与 IPFS

1.1 区块链技术

区块链来源于比特币，是对比特币底层技术的抽取，区块链本质上是一个对等网络（peer to peer, p2p）的分布式账本数据库^[3]。区块链是将区块和区块通过链式结构连接起来，每个区块中包含区块特有的一些信息和交易记录数据，它具有去中心化、交易公开透明、开放共识、数据无法篡改等特点。用户不需要了解对方身份就可以和对方进行交易，且交易一旦达成就会公开广播至全网的所有节点中，所有节点达成共识后将把该次交易记录复制到各自节点的账本中。因此，区块链网络中的每个节点都有一个完整的数据账本，要想修改区块链中的数据是十分困难的^[4]。

根据区块链的使用对象、准入规则、节点规模等可将区块链划分为公有链、联盟链、私有链三种类型^[5]。

公有链是完全去中心化的，任何互联网用户都能够随时加入并任意读取数据，能够发送交易和参与区块的共识过程，比特币和以太坊等虚拟货币系统就是典型的公有链系统^[6]。联盟链则是部分去中心化的，仅对特定的组织团体开放的区块链系统，典型的联盟链系统有超级账本^[7]和 EOS（enterprise operation system, 商用分布式设计区块链操作系统）等。而私有链则是中心化的区块链系统，由某个组织或机构控制的区块链，目前市场上尚未出现与用户业务应用直接相关的典型私有链应用^[8]。

1.2 智能合约

智能合约是运行在区块链之上的计算机协议，等价于一段事先被规定好逻辑和条款的计算机代码被激活运行的状态。它取代了传统的纸质合同，减少了在合约制定、控制协议和执行效率上的人工花费与计算成本^[9]。

智能合约通常都是预定义的，将各参与方的规定的业务逻辑化为机器可读的数字代码形式，运行在计算机网络中，用户之间无需第三方机构参与即可发生可信交易，减少了对中介的依赖，也提高了交易的安全性。

1.3 IPFS

IPFS 是一种点对点的分布式文件系统。它具有内容可寻址、版本化、点对点超媒体等特点，目标是补充甚至取代超文本媒体传输协议（hyper text transfer protocol, HTTP），构建更快、更安全、更自由的互联网时代^[10]。

IPFS 的基于内容寻址方式使得用户无需关心服务器位置、文件存储名字、文件路径等因素，当有文件上传至 IPFS 节点时，系统会基于文件内容计算出唯一的加密哈希值，此哈希值是代表文件内容的数字指纹，可验证文件内容是否被篡改，哪怕只修改文件的一个字符，哈希值也会

发生巨大变化。当有节点想下载某一文件时，只需输入文件哈希值，系统会根据分布式哈希表找到文件对应的位置，验证文件并将其取回。

2 基于联盟链的标准管理系统设计

2.1 系统设计思路

根据实际的操作流程，本系统应包含标准文件管理、联盟成员管理、标准投票共识、标准分享社区以及相应的数据查询共 5 大模块，由于系统包含联盟成员投票共识操作，这种分布式的多节点协同操作往往都存在信任问题，传统的中心化 Web 系统无法解决这一问题，采用数据库的存储方式也存在投票结果和标准文件被篡改的安全隐患，一旦联盟成员的账号泄露或是数据库受到攻击，很可能会对新标准有所影响，进而导致建筑在实际建设过程中遇到阻碍。

利用区块链结合 IPFS 可解决上述的一系列问题。区块链中的联盟链可将联盟组织成员以节点形式绑定，通过智能合约可验证节点身份和约束各节点的业务逻辑操作，且联盟链的每个节点都有一份相同的数据账本，使得系统的被攻击成本更高，具有更强的安全性。结合 IPFS 系统也能解决区块链账本无法存储文件的难题，提高了系统的存储性能。

2.2 系统的架构设计

本文提出的基于联盟链的建筑行业标准管理系统分为四层，分别为用户层、应用层、业务逻辑层和数据存储层，如图 1 所示。其中用户层分为联盟内的节点用户和联盟外的非节点用户，联盟内节点用户具有标准文件管理、发布投票、查询记录和管理分享社区后台等功能，而联盟外成

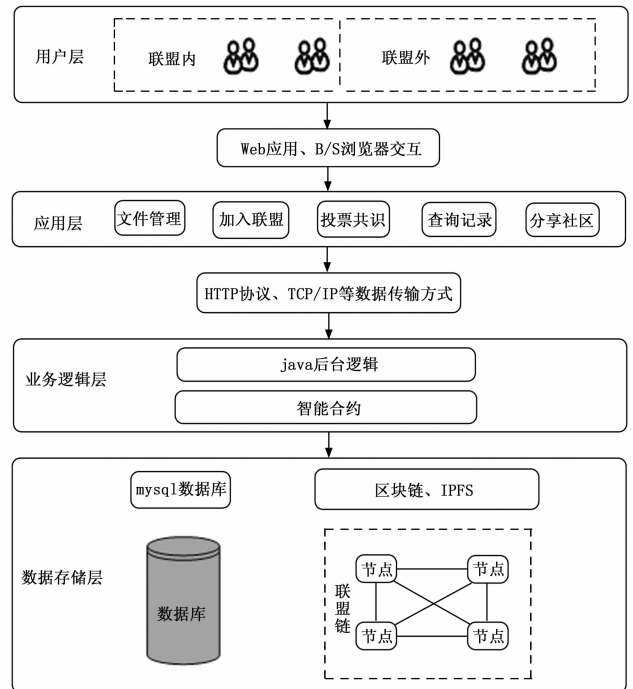


图 1 系统架构图

员又分两类,一类是想加入联盟成为标准参编单位的其它单位组织,另一类则是分享社区中的各建筑子公司成员,负责将标准在使用过程中的信息反馈给联盟链的标准参编单位。用户通过 B/S 架构的 Web 应用与应用层交互,在应用层完成相应的业务请求,并将对数据进行封装,通过 HTTP、TCP/IP 协议发送到业务逻辑层,在该层中完成相应数据业务操作,根据结果判断数据的存储位置,说通过后台服务器和智能合约将数据发送到数据存储层,最终将数据分别存储在数据库、区块链和 IPFS 中,区块链和 IPFS 系统都是以联盟链的形式连接,各节点间形成对等式网络结构^[11]。

通过此架构设计为系统划分了层次,优化了系统结构,各层之间相互独立又彼此协调,利用用户层赋予系统内不同用户不同权限,同时对外界用户进行隔离,而其它三层打通了客户端与数据底层之间联系,以应用层为操作起点,利用业务逻辑层处理及分发数据,完成数据在底层三端的存储,确保数据的安全性。

2.3 系统的业务流程分析

标准管理系统的整体流程如图 2 所示,具体流程如下:

1) 标准上传阶段:

标准上传阶段主要负责将某一联盟成员的标准上传到相应的数据库和 IPFS 系统中,当联盟中有成员完成对标准的编制或

上传日期、上传单位、标准版本和备注等记录信息上传到数据库中,同时标准文件自动上传到 IPFS 系统中,IPFS 会返回该文件唯一的加密哈希值,该哈希值作为文件的校验信息,将其也存入数据库中,其它节点可通过该哈希值在 IPFS 系统内下载该文件。

2) 标准共识阶段:

标准共识阶段主要分为发布投票内容和投票共识两个部分,首先由上传标准的节点用户发布投票,将标准文件版本、标准文件的加密哈希值、发布日期、发布人和发起投票请求等信息公布,在后台验证节点身份,通过后投票内容便发布成功,发起者通过系统内的邮件通知功能将新一轮的投票信息发送给该联盟内的所有节点用户。其它节点用户收到邮件后便进入投票共识流程,其它节点通过投票中的文件加密哈希值到从上传的 IPFS 节点中下载该文件,并通过文件验证模块验证文件内容是否和上传时一致,各节点需在智能合约所规定的时间内完成投票,投票结束后在智能合约判断投票是否通过,通过后便将投票结果和文件的加密哈希存入区块链和数据库,失败则只将投票结果存入数据库。

3) 标准应用阶段:

新标准一旦在联盟中达成共识,通过后台服务器会自动

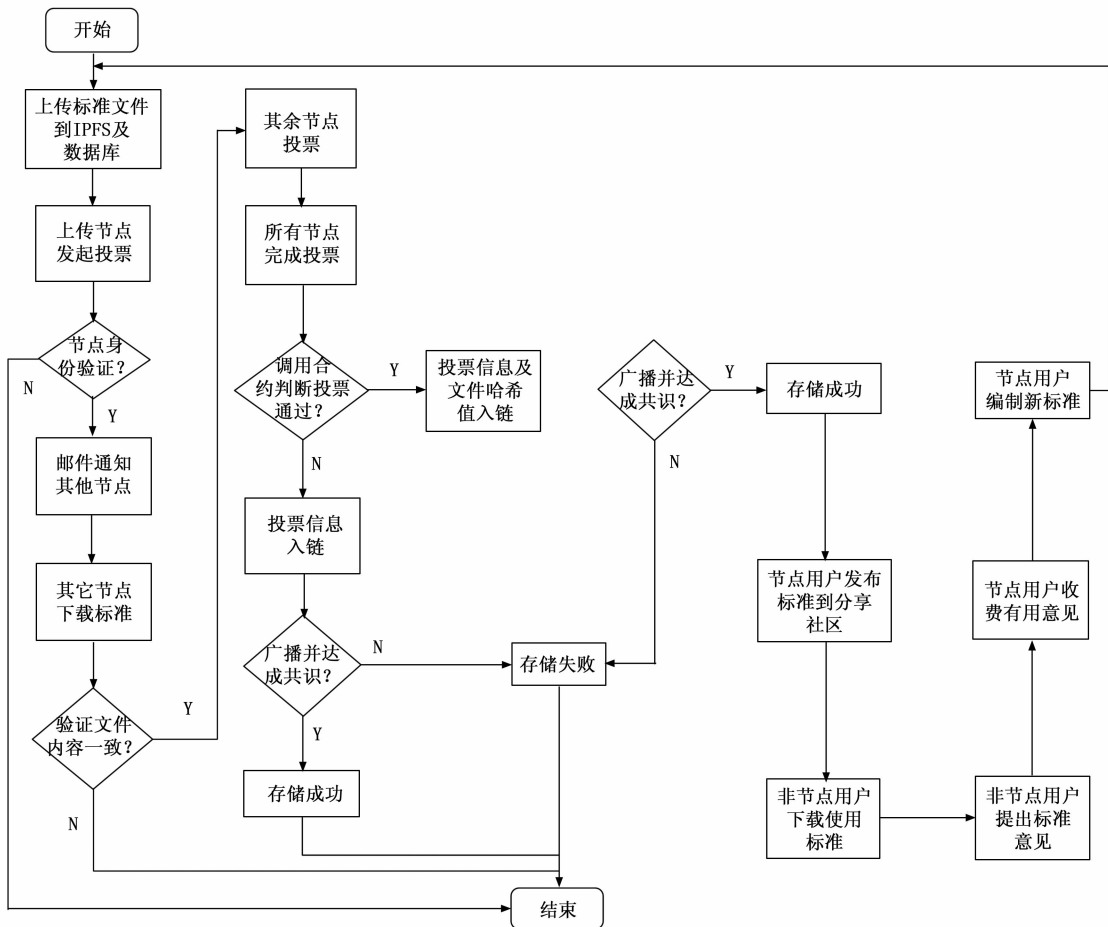


图 2 标准管理系统流程图

上传到系统的分享社区子系统中，并发布相应公告，供各大建筑子公司使用，由各建筑公司内部员工使用并在社区中各单位板块反馈意见，由相应的单位管理员收集本单位的有用反馈信息，定期将有用的反馈数据发布到对应标准版本的意见收集贴中，方便各联盟成员进行新一轮的标准编制。此外，系统还具有加入联盟和查询功能，若有其它想加入联盟组织的单位，可通过系统的加入联盟功能实现，在得到联盟组织所有节点用户的一致同意后，便可加入到联盟内部，参与具体的标准编制过程，并可在查询系统中查询相应投票结果、文件上传记录和联盟信息。

2.4 智能合约设计与区块链数据存储

根据智能合约的强制执行和去信任的特点，系统中涉及到多个节点的业务或是关键数据的存储都是由智能合约实现，例如节点身份验证、加入联盟、投票共识和查询系统等等，都是将其业务流程代码化，部署到联盟链的各个节点中，智能合约保证业务流程执行中的正确性，而区块链负责执行后的数据安全存储。

在区块链中只能存储类似于字符串的文本数据，无法保存文件类型的数据，所以采用分布式的 IPFS 文件存储系统保存文件，通过后台服务器建立 IPFS 与区块链之间的联系，区块链负责保存文件的加密哈希值，区块链、数据库和 IPFS 系统三端协同保证文件安全性，而其它结构化的文本数据则存储在数据库和区块链两端。

在本系统的联盟链中，涉及到数据存储的节点分为背书节点、排序节点和锚节点三类，其中背书节点负责验证交易，并对其进行签名，排序节点负责打包交易，保证交易的顺序，锚节点负责各节点之间的通信。区块链的数据存储过程如图 3 所示，首先由背书节点调用客户端发起交易，背书节点模拟执行交易，将交易和执行结果打包，验证后发给客户端，当所有背书节点对交易进行背书签名后，将打包后的数据发送给排序节点进行共识排序，生成新区块后将结果发送给联盟通道中的所有节点，更新在各节点账本中，保证各节点的一致性。

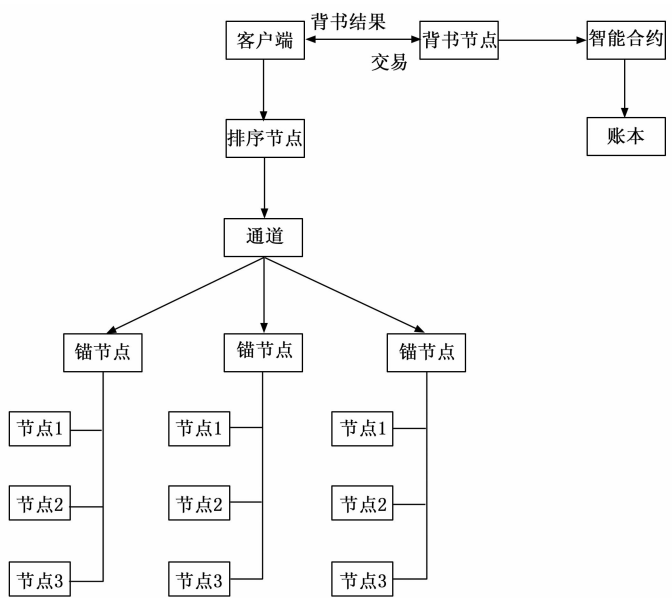


图 3 区块链节点的数据存储过程

3 标准管理系统的实现

本文基于上述系统设计，实现了一个基于联盟链的建筑行业标准管理系统，系统功能模块如图 4 所示，本系统在 Hyperledger Fabric 平台搭建联盟链，系统共有 26 个联盟链节点和 IPFS 节点，实现了区块链和 IPFS 的去中心化存储功能，并结合 Java 语言开发 Web 管理系统。系统共包含区块链、IPFS、标准管理系统三个后台子系统，IPFS 与标准管理系统后台采用 Java 语言编写，而区块链后台由 Go 语言开发的智能合约控制，可由上层的 Java 后台发起调用智能合约请求。本系统的区块链采用 Kafka 共识机制，该算法通过排序节点接收联盟链内的交易，并对其进行排序，执行完交易后将交易结果保存在排序节点的本地日志中，最后利用 p2p 传播方式将结果扩散给联盟链的每个节点。系统共包含文件管理、加入联盟、投票共识、查询记录和分

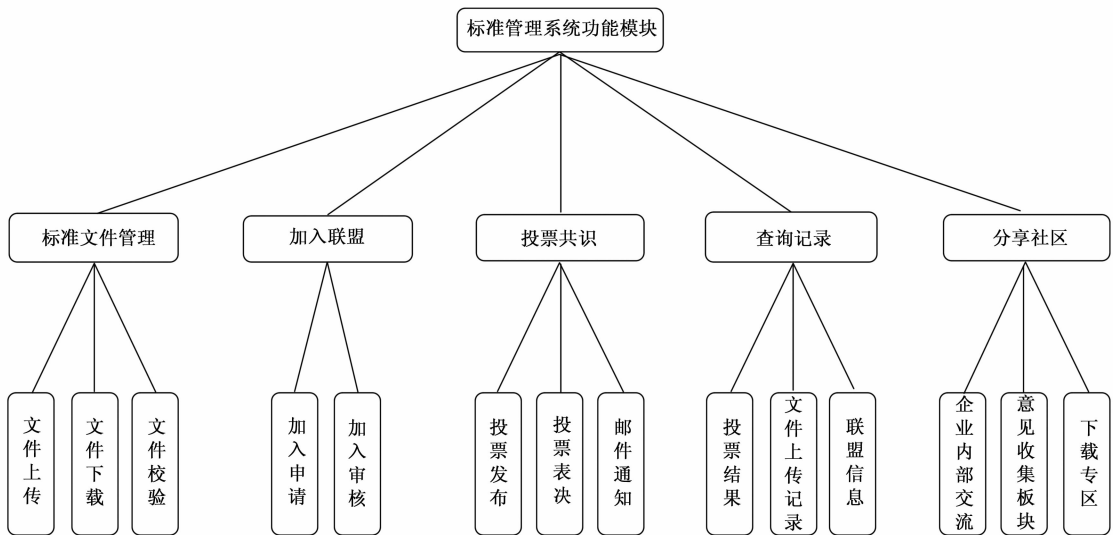


图 4 系统功能模块

享社区 5 大模块。3 个后台同时运转, 各接口相互调用保证系统的正常运行以及数据的三方协同。

先在 Linux 系统下搭建 Hyperledger Fabric 开发环境, 安装 Go 语言、Git 及 Docker 相关组件, 下载 Fabric 源码并进行编译, 然后在 configtx.yaml 配置文件中设置联盟节点信息, 定义区块链网络组织结构及创世区块, 在区块链网络中选择适合多节点的 Kafka 算法作为共识机制, 对网络进行初始化后即可启动网络。然后在同样环境下搭建 IPFS 节点集群, 下载 IPFS 安装包并进行解压, 对 IPFS 节点进行初始化并创建节点信息, 搭建完多节点集群后输入 ipfs daemon 启动 IPFS 网络。底层环境搭好后便可在其上开发相应功能。

标准文件管理模块包含文件上传、文件下载和文件校验 3 个子功能, 标准文件上传界面如图 5 所示, 节点用户录入文件、上传单位、上传日期、上传版本和备注等相应信息后, 文件会上传到 IPFS 系统, IPFS 经过特定算法后会返回一个以 Qm 开头的 46 位文件哈希值, 后台将该文件哈希与其他的文件上传信息存入数据库中, 其它节点用户可根据该文件哈希在此模块中下载或校验文件。



图 5 标准上传

用户上传新标准文件后, 需在系统内发布相应的投票内容, 利用邮件通知联盟内各成员后, 各用户在智能合约规定的 2 天内完成投票, 投票表决界面如图 6 所示, 利用投票合约在后台绑定每个用户节点身份, 通过智能合约判定用户投票是否有效, 当某一节点用户投票后, 投票合约会调用相应的投票统计合约进行统计, 达成投票结束条件时, 该合约会自动统计投票赞成数是否超过三分之二, 并给出文件信息是否入链的响应。



图 6 投票表决

分享社区子系统界面如图 8 所示, 该子系统采用 Java 中的 MVC (model view controller, 模型-视图-控制器) 设计模式和三层架构的开发方式, 嵌入至本标准管理系统中, 主要给各建筑子公司等施工单位的非节点用户使用, 负责提供标准实施过程中的使用数据, 与节点用户建立服务通道, 解决标准更新机制缓慢的问题。用户可在分享社区子系统中下载相应标准, 并在各自的单位内部交流讨论, 发表并查看内部的帖子和评论等, 联盟链的节点用户在分享社区子系统中是超级管理员身份, 具有相应的删除功能, 收集意见的同时也需维护分享社区的秩序。



图 7 查询投票结果



图 8 分享社区子系统

4 结束语

本文设计并实现的系统对标准进行了生命周期管理, 信息化的标准管理方式和区块链的共识机制提高了标准管理的效率, 利用联盟链和智能合约解决了标准共识过程中的身份信任问题, 区块链系统去中心化存储也提高了系统的安全性, 结合 IPFS 解决区块链无法存储文件的难题, 将文件存储在 IPFS 分布式文件管理系统中, 在区块链端存储文件的数字指纹, 进一步保证标准件的权威性。目前系统整处于测试运行阶段, 整体运行良好, 但有联盟外单位加入联盟链时, 智能合约无法实现智能更新联盟链的节点用户数量, 各单位需要关闭区块链, 在联盟中更新智能合约后重启方可生效, 未来将考虑在智能合约中实现自动更新新加入的节点信息, 进一步优化系统的扩展性。

(下转第 230 页)