

基于区块链技术的数字电影流动放映系统*

陈冰容¹, 张延华¹, 孙恩昌¹, 李萌¹, 杨奎²

(1.北京工业大学 信息学部, 北京 100124; 2.联通系统集成有限公司, 北京 100176)

摘要: 针对目前数字电影流动放映集中式管理中的安全与信任问题, 提出一种基于区块链技术的数字电影流动放映系统架构。以区块链技术的去中心化共识机制和 IPFS 数据分布式存储机制保障数据的可信和可追溯, 采用区块链智能合约脚本设计影片交易、授权认证、放映监管等环节的业务逻辑, 融合数据存储机制和数据地址记录, 在版权方、院线、放映队、数字节目管理中心、监管部门间达成分布式共识, 形成高效准确的执行, 减少交易和授权中的人为干预性, 从而保证流动放映操作全程可控。

关键词: 区块链; 智能合约; IPFS; 流动放映

中图分类号: TN91; TP311.13

文献标识码: A

DOI: 10.16157/j.issn.0258-7998.191225

中文引用格式: 陈冰容, 张延华, 孙恩昌, 等. 基于区块链技术的数字电影流动放映系统[J]. 电子技术应用, 2020, 46(8): 107-111.

英文引用格式: Chen Bingrong, Zhang Yanhua, Sun Enchang, et al. Digital movie mobile playing system based on blockchain technology[J]. Application of Electronic Technique, 2020, 46(8): 107-111.

Digital movie mobile playing system based on blockchain technology

Chen Bingrong¹, Zhang Yanhua¹, Sun Enchang¹, Li Meng¹, Yang Kui²

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

2. Unicom Systems Integration Co., Ltd., Beijing 100176, China)

Abstract: To solve the security and trust issues in the centralized management, an architecture of digital movie mobile playing system based on blockchain technology is proposed, which provides the credibility and traceability of data by the decentralized consensus mechanism of blockchain and the distributed storage mechanism of IPFS. Here, smart contracts are used to realize the execution logic for the specific functions in the movie mobile playing, including film trading, authorization certification, screening supervision, etc., which integrate the data storage and address record, and reach distributed consensus among copyright owners, cinemas, projection teams, digital program management centers and regulatory departments. This automatically execution with efficiency and accuracy reduces the artificial intervention in transactions and authorizations, and therefore the fully controllable operation of mobile playing is guaranteed.

Key words: blockchain; smart contracts; IPFS; mobile film projection

0 引言

流动电影放映是加强乡村文化建设, 满足人民群众日益增长的精神文化需求的一项重点文化工程。目前针对流动电影的管理一般都是基于传统集中式数据库技术的数字电影流动放映系统(Digital Movies Mobile Playing System, dMs)系统^[1-2]。随着流动电影放映工作的推进, 这种“中心化”的管理模式暴露出许多问题^[3-4]。首先, 存在虚报放映数据, 套取政府补贴的现象; 其次, 中心数据库存在数据存储安全性问题; 最后, 影片版权保护不足, 违法者通过盗版播放或传播手段获利。

区块链(Blockchain)作为一种去中心化的分布式账本技术, 拥有安全透明、可追溯、不可篡改等特点, 为基于区块链的各种应用提供了安全可靠的信任和存储机制^[5-6]。例如, 利用区块链的特性, 出现了政务、商务和法务信息的追溯, 使各个环节产生的数据可靠、可信^[7]; 在通用平台研究方面, 有人提出去中心化的个人数据管理系统用于实现存储、查询和数据共享, 从而确保用户能够拥有和控制自己的敏感信息^[8]; 还有人提出并实现了去中心化的农产品溯源系统, 用溯源二维码为消费者提供安全、可靠、真实的农产品溯源信息^[9]。

* 基金项目: 国家自然科学基金资助项目(61571021, 61901011); 北京市博士后工作经费资助项目(ZZ2019-73); 中国博士后科学基金第 64 批面上项目(2018M640032); 北京市教委科技计划项目(KM202010005017); 朝阳区博士后科研活动经费资助项目(2019ZZ-4)

本文针对流动电影放映管理系统中数据的可信问题,提出一种基于区块链技术的流动放映系统架构,通过区块链智能合约及 IPFS,保证流动放映数据在影片交易、授权认证、放映监管等各个环节中不可篡改,为流动放映提供操作的可审计性。

1 区块链技术及应用特性

1.1 区块链定义

区块链本质上是一个对等网络(Peer to Peer, P2P)的分布式账本,是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式^[10]。它使用链式区块来检验和存储数据,使用密码学来保证数据的安全与完整,使用共识机制保障账本数据在全网中形成正确、一致的共识,使用可编程的智能合约来实现自动化操作^[11]。与传统数据存储相比,区块链技术具有去中心化、公开透明、不可篡改、可追溯等特点。

1.2 智能合约

智能合约是一类计算机协议,它们一旦制定和部署就能实现自我执行和自我验证,而且不需要人为干预。区块链技术的发展促使了智能合约的发展^[12]。

1.3 IPFS

星际文件系统(InterPlanetary File System, IPFS)是一个对等的分布式文件系统^[13]。它结合分布式散列表、鼓励块交换和一个自我认证的名字空间。IPFS 没有单点故障,并且节点不需要相互信任。

2 区块链和 IPFS 的流动放映系统架构设计

基于区块链和 IPFS 的流动电影放映系统需要满足流动电影放映环节中关键信息的安全存储和授权访问,包括一系列控制流动电影放映过程的信息,如影片交易数据、授权数据、放映数据等。对于不同的关键信息,用户有不同的权限和共享策略。鉴于区块链存储容量有限,系统中关键信息经加密后进行链下存储,而区块链只存储关键数据的哈希值。由于区块链与 IPFS 的兼容性较好,本系统采用 IPFS 作为链下存储数据库^[14]。

去中心化的区块链流动放映系统架构设计如图 1 所示,由应用交互层、数据服务层和数据接入层构成。

2.1 应用交互层

应用交互层包括系统的基础功能模块,支持 B/S 架构,用来实现流动放映系统的核心业务逻辑,为用户提供操作服务,可由 WebApp 实现用户与区块链和 IPFS 层的交互,包括使用 WebApp 进行相应操作后调用智能合约。

2.2 数据服务层

数据服务层由区块链 P2P 网络和 IPFS 网络共同组成,以确保所有区块节点都可以参与到数据信息的传输校验过程中。基于区块链和 IPFS 的存储模型如图 2 所示,其中每个矿工检查接收到的事务,将有效事务放入交易池中,并存储在 IPFS 中,同时返回事务的 IPFS 哈希

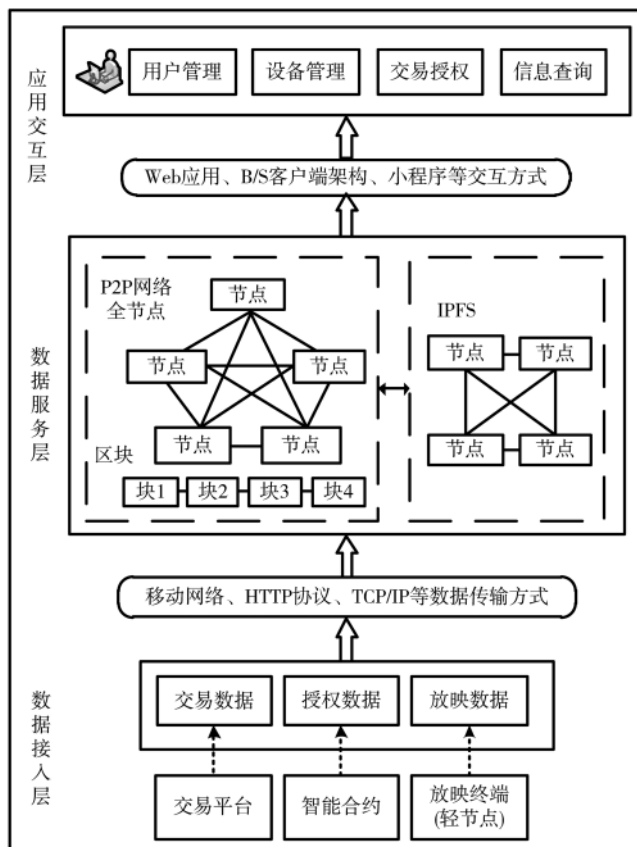


图 1 系统架构图

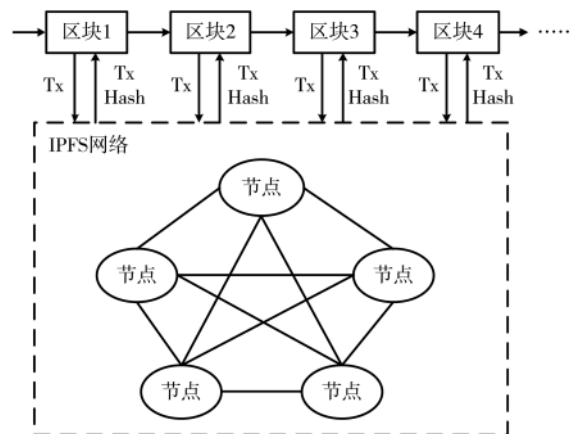


图 2 基于区块链和 IPFS 的存储模型

值。当计算下一个块时,每个矿工将验证过的 IPFS 哈希打包到新的区块中并计算 merkle 根和区块哈希。

因此,IPFS 负责存储加密后的信息,并返回哈希。区块链负责存储智能合约代码和执行智能合约,并将执行结果打包成区块,经过共识后写入区块链账本。区块链网络中的各个节点组成区块链联盟体,内部维持共识机制,为系统交易的验证和存储提供服务。而由于 IPFS 网络去中心化和基于内容寻址的特性,用于存储大文本数据,例如授权文件,文件内容的哈希值存储于区块链中。

计算机技术与应用 Computer Technology and Its Applications

2.3 数据接入层

数据接入层是流动放映系统的物理区域和基础模块。该层一般利用物联网传感器、通信等技术采集必要数据,通过区块链接口调用数据上传智能合约将数据存储至区块链,保证数据来源可靠、可信。

3 系统业务流程分析和智能合约设计

3.1 系统业务流程分析

与流动电影放映相关的系统业务有 5 类,分别为版权方、院线、放映队、数字节目管理中心、监管部门。这 5 类用户接入区块链作为 P2P 用户节点,分布式存储的区块链会在每个用户节点产生信息备份,以此形成用户交互的信息网络。图 2 数据接入层中的放映终端设备为内嵌区块链轻量级节点模块的放映机,作为区块链轻节点参与信息交互。流动电影放映全流程如图 3 所示,分为 3 个阶段:影片交易、授权分发、信息回传。

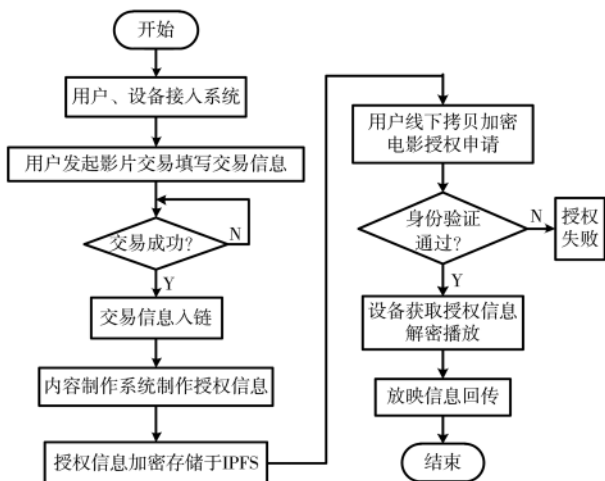


图 3 流动电影系统流程

用户和放映设备注册后,订购方向版权方发起影片交易,交易成功后内容制作系统制作加密影片并根据相应的信息生成授权信息。放映员线下拷贝相关影片,放映之前进行授权申请,进行相关身份认证后,授权信息会发送到对应区块链放映机轻节点进行授权放映。区块链轻节点在放映完成后会自动上传放映信息至区块链,以便管理方监管具体放映情况。

3.1.1 影片交易

影片交易主体为版权方和订购方。版权方作为卖方提供片源、制定影片价格。订购方既可以是放映员个体,也可以是院线并且根据版权方提供的片源进行影片订购。双方通过影片交易服务平台进行影片交易,基本业务处理逻辑主要为订购方发送交易请求,交易后台响应并转发交易请求到区块链服务器。区块链服务器接收并广播交易,在各个区块链节点达成共识后记入区块链账本并向交易后台返回交易结果,成功后向用户返回最终交易结果,具体业务处理逻辑如图 4 所示。

3.1.2 授权分发

版权方和订购方交易成功后,区块链中存储了交易的详细信息,包括购买的影片信息、影片放映设备信息、放映员信息等。影片制作系统制作加密影片并根据交易信息生成相应的授权信息,并将授权信息加密存入 IPFS 中。授权信息含加密影片解密播放的密钥。为监管加密影片在指定合法放映的设备上播放,系统通过交易信息中的影片放映设备信息检索得到区块链放映机注册时产生的公钥,然后用设备公钥对授权信息进行非对称加密。当订购方用户向版权方用户进行授权申请时,首先需要通过身份认证,授权信息的哈希值将会通过交易广播给区块链网络,只有拥有设备私钥的区块链放映机才

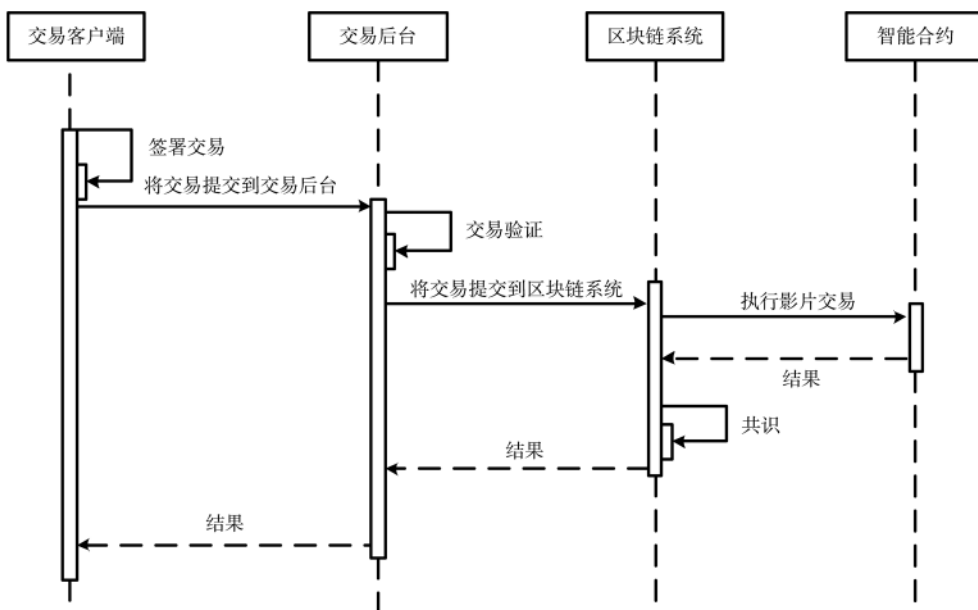


图 4 影片交易业务逻辑

可解密获得授权信息,然后下载授权信息至设备中进行相应的影片解密工作。

(1) 用户注册

用户使用 WebApp 输入用户 ID、密码,并选择用户类型后发起注册请求。WebApp 验证提交的信息后根据输入的密码生成用户公钥和私钥以及区块链地址,同时向区块链节点请求调用用户注册合约 Register_Contract.UserRegister 完成用户注册请求,并广播至各块链节点,达成共识并记账后用户注册完成。

(2) 设备注册

设备生产商使用 WebApp 登录,填写设备信息进行设备注册,WebApp 验证提交的设备信息后根据输入的设备唯一序列号生成设备公钥和私钥以及区块链地址,同时向区块链节点调用设备注册合约 Register_Contract.DeviceRegister 完成设备注册请求,并广播至各块链节点,达成共识并记账后设备注册完成。

(3) 授权信息上传

版权方用户使用 WebApp 上传信息并用用户的公钥对上传请求进行签名,然后将授权信息用设备公钥进行加密后存入 IPFS 中并获取 IPFS 返回的哈希值,同时向区块链节点请求调用数据存储合约 Data_Contract.SaveInfo,区块链节点接收到请求首先验证用户的签名,通过后执行智能合约,并将哈希值、信息类型进行全网广播,达成共识后将智能合约执行结果写入区块链中,授权信息上传流程如图 5 所示。

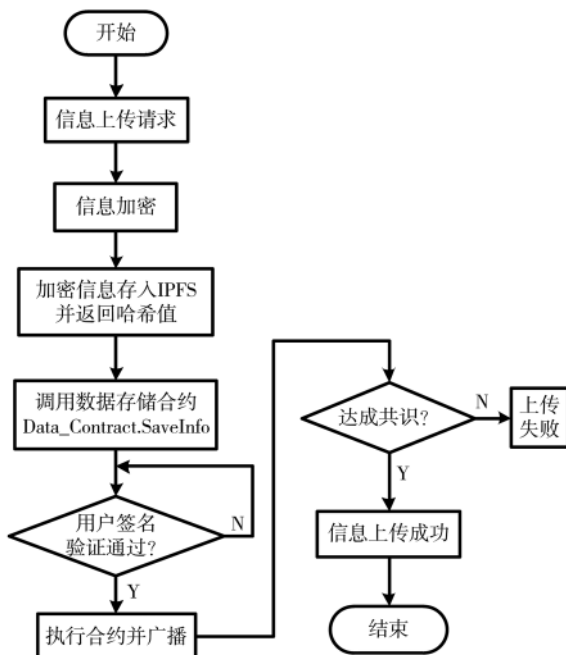


图 5 信息上传流程图

(4) 授权信息查询

信息查询流程如图 6 所示。订购方用户可根据需要进行查询操作,用户发起查询请求进行签名后 WebApp

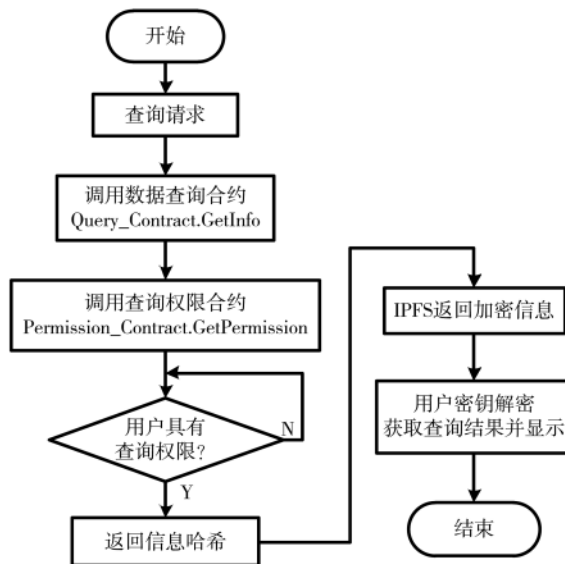


图 6 信息查询流程图

提取查询信息类别,然后向区块链节点请求调用数据查询合约 Query_Contract.GetInfo 输入用户 ID 和信息类别,区块链节点验证用户的签名后执行智能合约 Query_Contract.GetInfo,然后继续调用查询访问权限合约 Permission_Contract.GetPermission,区块链节点智能合约根据用户信息及查询信息判断是否具有查询权限,若有权限则相应的区块链放映机轻节点调用区块链查询接口获取查询信息的哈希值,然后根据哈希值获取 IPFS 节点存储的加密信息。

3.1.3 信息回传

放映员完成相应的影片放映工作后,区块链轻节点放映机将信息回传作为交易请求,调用信息回传智能合约并将交易请求发送至区块链服务器。区块链服务器接收并广播交易,在区块链节点达成共识后记入区块链账本并向用户返回信息回传结果,具体业务处理逻辑如图 7 所示。

3.1.4 权限管理

系统用户访问信息均需提交用户信息向区块链节点请求调用权限管理合约 Permission_Contract.SetPermission,区块链验证用户的签名并执行智能合约后将请求进行全网广播,达到共识后允许用户进行下一步操作。

3.2 智能合约设计

系统中的智能合约脚本根据系统功能设计,例如根据用户注册、关键数据上传、授权访问等业务流程进行设计并部署在区块链网络中,用户进行操作以及调用智能合约时由区块链网络节点进行共识。本系统根据不同功能设计了相应的智能合约,如表 1 所示。

系统流程的区块链智能合约的伪代码描述:

输入:影片交易信息、用户授权申请信息;

输出:如果信息校验成功,完整信息存入区块链;如

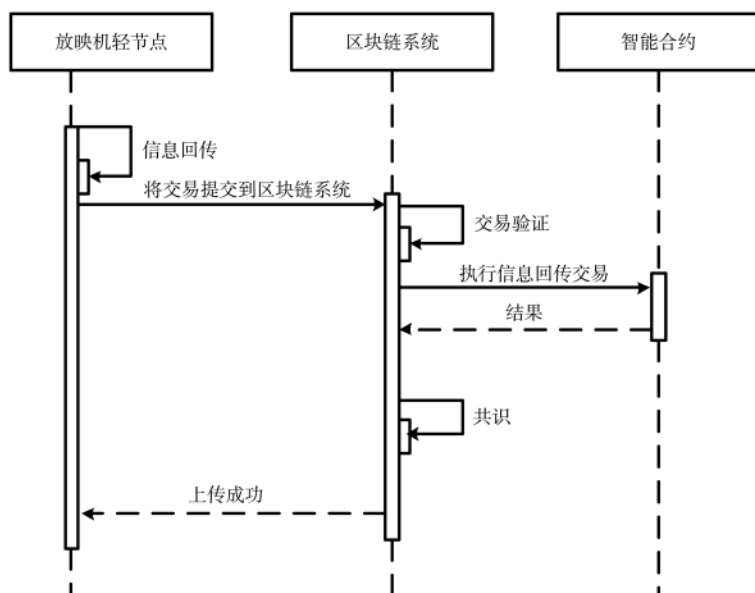


图7 信息回传业务逻辑

表1 智能合约接口

合约名称	接口定义	接口描述
注册合约 Register_Contract	UserRegister	用户注册
	DeviceRegister	设备注册
权限管理合约 Permission_Contract	SetPermission	授予访问权限
	GetPermission	查询访问权限
	CancelPermission	撤销访问权限
数据存储合约 Data_Contract	SaveInfo	信息入链
数据查询合约 Query_Contract	GetInfo	信息查询

果信息校验失败,返回错误信息。

- (1)编译影片交易智能合约 or 授权申请智能合约
- (2)部署智能合约并调用 start()
- (3)解锁已有账户 Account
- (4)获取输入信息
- (5)If 影片交易校验失败 or 授权申请校验失败
- (6)Return error
- (7)Else

实例化数据存储智能合约 Data_Contract.SaveInfo()

(8)End

4 结论

数据存储与信任问题一直是流动电影放映管理中难以解决的问题,信息安全可靠的存储以及授权信任机制无法得到保障时整个流动放映系统将无法保证放映质量。而区块链技术以其分布式结构和共识机制为数据存储和授权提供可信性保证。本文设计的基于区块链的流动放映系统架构以区块链支撑版权方、院线、放映队、数字节目管理中心、监管部门等多个用户节点间的可信交易管理,以智能合约形式完成具体的流动放映全程的数据安全可靠存储和操作记录以及授权信任机制防止非授权的访问和操作。

《电子技术应用》2020年 第46卷 第8期

参考文献

- [1] 鲍林岳.数字电影流动放映系统(dMs)简介[J].现代电视技术,2005(12):30-32.
- [2] 鲍林岳.数字电影的信息化交易、服务和管理[J].现代电影技术,2009(6):3-8.
- [3] 陈彤.提高数字电影流动放映质量应注意的问题[J].现代电影技术,2016(8):56-58.
- [4] CARVALHO A.A. a permissioned blockchain-based implementation of LMSR prediction markets[J]. Decision Support Systems, 2020, 130: 113228.
- [5] 贡佳伟,陈君,曾学文,等.数字电影流动放映系统安全体系的设计[J].微计算机信息,2009,25(18):27-29.
- [6] 陈宇翔,郝尧,赵越,等.基于区块链的版权保护方法研究[J].电子技术应用,2019,45(10):25-28.
- [7] 任明,汤红波,斯雪明,等.区块链技术在政府部门的应用综述[J].计算机科学,2018,45(2):1-7.
- [8] ZYSKIND G, NATHAN O, ALEX S P. Decentralizing privacy: using blockchain to protect personal data[C]. IEEE Security and Privacy Workshops. IEEE Computer Society, 2015: 180-184.
- [9] 张延华,杨兆鑫,杨睿哲,等.基于区块链的农产品溯源系统[J].情报工程,2018,4(3):4-13.
- [10] 邓柯.区块链技术的实质、落地条件和应用前景[J].深圳大学学报(人文社会科学版),2018,35(4):53-61.
- [11] 王晓光.区块链技术共识算法综述[J].信息与电脑(理论版),2017(9):72-74.
- [12] 贺海武,延安,陈泽华.基于区块链的智能合约技术与应用综述[J].计算机研究与发展,2018,55(11):112-126.
- [13] NIZAMUDDIN N, SALAH K, AJMAL M, et al. Decentralized document version control using ethereum blockchain and IPFS[J]. Computers and Electrical Engineering, 2019, 76: 183-197.
- [14] 郝锦涛.基于 IPFS 的分布式电商系统的研究与实现[D].北京:北京邮电大学,2019.

(收稿日期:2019-11-13)

作者简介:

陈冰容(1995-),女,硕士,主要研究方向:区块链技术、数据挖掘技术。

张延华(1960-),男,硕士,教授,主要研究方向:工业互联网、区块链技术、智慧无线通信网络。

杨奎(1982-),通信作者,男,硕士,工程师,主要研究方向:政务区块链、智慧政务, E-mail: 15611028062@qq.com。

版权声明

经作者授权，本论文版权和信息网络传播权归属于《电子技术应用》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、DOAJ、美国《乌利希期刊指南》、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《电子技术应用》编辑部

中国电子信息产业集团有限公司第六研究所