

# 基于区块链技术的土建工程项目管理平台

左康达,孙知信

(南京邮电大学 现代邮政学院,江苏 南京 210003)

**摘要:**每个土建工程项目其工程浩大,流程复杂,且偷工减料、以次充好、造假数据、权钱交易获得工程承包权等暗箱操作事件时有发生。因此加强并完善土建工程项目的管理体系对土建工程顺利开展,提高工程的整体质量具有重要意义。区块链技术的去中心化、去信任、信息透明、数据不可篡改可溯源等特征可一定程度上提高工程项目的安全性、降低工程事故的发生率。针对当前土建工程项目管理的痛点,文中提出了一种基于联盟区块链的土建工程项目管理平台 CEPM-Chain,探索了智能合约应用以及将该技术与土建工程信息建模和信息管理相结合的可行性,利用区块链技术提高土建工程行业项目管理的流程效率。阐述了该系统的架构设计,并介绍了共识层的优化设计,采用节点角色分工、信誉度机制、随机话语权增加等方法降低其通信复杂度,提高其可扩展性,优化了该系统的性能。

**关键词:**区块链;土建工程;项目管理平台;智能合约;共识机制

中图分类号:TP39

文献标识码:A

文章编号:1673-629X(2021)12-0187-06

doi:10.3969/j.issn.1673-629X.2021.12.031

## A Civil Engineering Project Management Platform Based on Blockchain Technology

ZUO Kang-da, SUN Zhi-xin

(School of Modern Post, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

**Abstract:** Each civil engineering project has a huge amount of engineering, complicated processes, and black-box operations such as cutting corners, shoddy materials, falsifying data, and obtaining engineering contracting rights through rights and money transactions, etc. happen from time to time. Therefore, strengthening and perfecting the management system of civil engineering projects is of great significance to the smooth development of civil engineering projects and improving the overall quality of the project. The characteristics of blockchain technology such as decentralization, trustlessness, information transparency, and non-tamperable and traceable data can improve the safety of engineering projects and reduce the incidence of engineering accidents to a certain extent. Aiming at the current pain points of civil engineering project management, we propose a civil engineering project management platform CEPM-Chain based on alliance blockchain, exploring the feasibility of application of smart contracts and combining it with civil engineering information modeling and information management, and using blockchain technology to improve the process efficiency of project management in the civil engineering industry. The architecture design of the system is explained, and the optimization design of the consensus layer is introduced. The method of node role division, reputation mechanism, random voice increase and other methods are used to reduce the communication complexity, improve its scalability, and optimize the performance of the system.

**Key words:** blockchain; civil engineering; project management platform; smart contract; consensus mechanism

## 0 引言

土建工程是一个相对广泛的项目,是建筑工程与土木工程的结合,在实际的土建工程项目中包括多种类型,包括房屋建设、公路建设,还有其他的一些基础设施建设<sup>[1]</sup>。近年来,中国土建工程事业飞速发展,而

每个土建工程项目都是一个浩大的工程,其流程复杂繁琐。在每个土建项目的规划、建设和实施的部分中,任何一个流程的小错误都会造成严重后果且土建工程行业在巨大的体量下存在着大量黑箱流程<sup>[2]</sup>。土建工程项目事故频发,究其原因大多是工地在材料的进场

收稿日期:2020-11-30

修回日期:2021-03-30

基金项目:国家自然科学基金资助项目(61972208,61672299)

作者简介:左康达(1995-),男,硕士,研究方向为区块链技术、大数据技术及智慧物流等;孙知信,博士,博导,科技部评审专家、国家自然科学基金评审专家、教育部基金评审专家,江苏省科技成果评审专家,研究方向为计算机网络及安全、物联网应用、多媒体通信、计算机软件等。

验收和使用管理上没严格把关以及相关负责人员的渎职。细细分析相关工程事故,建筑材料的质量参差不齐、偷工减料、以次充好、造假数据、权钱交易获得工程承包权等暗箱操作事件屡现不止<sup>[3]</sup>。

传统的土建工程管理方式主要是人工管理,可随着土建工程的发展,人工管理的方式显现出许多问题,首先,人工管理难以保证土建工程管理工作的及时性和准确性;其次,人工管理的成本比较大,直接影响到土建工程的经济效益<sup>[4]</sup>;三是人工管理方式人为可操作空间大,容易篡改合约与数据,进行黑箱操作,滋生腐败。因此每个土建工程项目都急需一个可信的专门的监督或管理体系<sup>[5]</sup>。

中国的大多数土建工程项目是由国有企业持有的。在实际的投资建设过程中,大部分是由国有企业和有关政府部门管理和控制的<sup>[1]</sup>。无论规模和复杂性如何,土建工程项目主要是公司间的协作任务。土建工程是一个拥有大量数据和高度信任需求的领域,它通常需要多个参与单位和部门的协调与合作。相互交流应建立在高度信任的基础上,工作过程也需要对大量资源进行监督和控制<sup>[6]</sup>,其签订的合约与相关数据信息也需确保不可篡改,真实有效并全程可追溯,区块链技术具有的去中心化、去信任、信息透明、数据不可篡改可溯源等特性及应用场景特征与土建工程领域当前需求高度契合。利用区块链技术让工程项目从立项到竣工的每个环节各方参与者都严格监督,保存相关真实数据并无法篡改,则每个环节的参与者各司其职,严格按照工程要求进行,若出现工程事故,可第一时间找到相关原因及负责人。则必定可以提高工程项目的安全性,降低工程事故的发生率。

区块链联盟链现在大多以 PBFT 拜占庭容错算法作为它的共识机制。但它的可扩展性也相对较低,通信复杂度太高。通常,系统中的节点数接近 100 时,性能下降非常快的弊端让其实用性降低,解决这些弊端对于联盟链的发展尤为重要。文中提出的基于区块链技术的土建工程项目管理平台 CEP-Chain 将采用节点角色分工、信誉度机制、随机话语权增加等方法来减少上述弊端。

## 1 相关技术

### 1.1 区块链概述

区块链是分布式数据存储、共识机制、对等传输、加密算法和其他计算机技术的一种新的应用模型。区块链是结合了加密技术的分布式账本的应用。经过 30 多年的发展,由于智能合约的出现和发展,其应用也得到了极大的扩展,智能合约已从普通分类账转变为具有自动化功能的分类账本<sup>[7]</sup>。广义区块链技术是一种新的分散基础设施和分布式计算范例,它应用密码块结构来存储并且验证数据,更新以及生成数据使用分布式节点一致性算法来完成,使用智能合约来编程和处理数据。

区块链的特征有开放性、去中心化、独立性、匿名性、安全性、开放性,区块链技术基于开源。除了加密交易双方的私人信息外,区块链的数据还向所有人开放,整个系统的信息高度透明。去中心化,区块链中每个节点都实现了信息的自我传输、验证以及管理,没有中央控制。独立性,根据共识规范和协议,整个区块链系统不依赖第三方。所有节点无需其他人工干预便可以自动安全地验证和交换系统内的数据。匿名性,除法律法规要求,否则不必公开或验证每个块节点的身份,可以匿名传输信息。安全性,在控制所有数据节点的 51% 之前,无法操纵和修改网络数据,可避免主观和人为数据更改,使得区块链本身相对安全<sup>[8]</sup>。

2019 年 1 月 10 日,国家互联网信息办公室发布《区块链信息服务管理规定》<sup>[9]</sup>。2019 年 10 月 24 日,习近平总书记在中央政治局第十八次集体学习时强调,“把区块链作为核心技术自主创新的重要突破口<sup>[10]</sup>”。区块链已经进入公众视野,成为社会关注的焦点。

### 1.2 联盟链与共识机制

区块链可以分为公有链、联盟链、私有链,这取决于它们的安全级别和访问/成员限制。对比如表 1。联盟链,仅针对特定的成员组并限于第三方,该节点内部指定了多个节点作为记账节点,用于决定每个块的生成,其他节点有权限参与交易,但不参与记账<sup>[11]</sup>。

表 1 区块链类型对比

比较内容	公有链	联盟链	私有链
中心化程度	去中心化	多中心化	中心化
参与者	任何人	设定的成员	指定参与者
共识算法	POW、POS 等	PBFT 等	自行背书
代表应用	比特币、以太坊	超级账本	多链
优点	去中心、开放安全	可控性强、延展性高、提高隐私保护	速度快、成本低
缺点	速度慢、成本高	未完全解决信任问题	存在信任问题

“共识机制”是通过共识节点的表决,在短时间内完成交易的验证以及确认;如果许多不相关的节点可以达成交易协议,便可假设整个网络也可达成协议<sup>[12]</sup>。常见的共识机制包括:POW(工作量证明机制)、POS(权益证明机制)、POW+POS(混合共识机制)、DPOS(股份授权证明)、PBFT(拜占庭容错算法)。联盟链主要采用的是PBFT算法,但现有实用拜占庭容错算法(PBFT)在联盟链应用场景下存在扩展性差、通信开销大、效率低等问题。

### 1.3 数字签名与智能合约

#### (1) 数字签名。

哈希函数,区块链的链结构以及共识机制可以确保不会篡改写入区块链总账的数据,而基于非对称加密技术的数字签名可避免假账等的发生。解决信任问题的最简单方法是在每个条目上附加一个无法冒充的签名。通过签名,任何人都可以确认谁是账户的发起人,从而通过历史数据来验证账户的合法性,若验证未通过,则不会记录在账户中<sup>[13]</sup>。

椭圆曲线算法和RSA等典型的非对称加密是一项极为重要和有效的安全技术,区块链使用该技术来实现数字签名。非对称加密方法用于生成一对公钥和私钥:公钥暴露给整个区块链以进行笔迹验证。私钥由用户持有,用户可以使用私钥在他希望记录到区块链的账户上签名<sup>[14]</sup>。

#### (2) 智能合约。

智能合约是Szabo于1994年首次提出的。它的概念是:在计算机系统中,当执行某些交易时,可以触发相应的代码以自动执行,并可以生成相应的输出合约。但是,由于难以确保智能合约的代码不被篡改,因此其实际应用受到很大限制。随着区块链技术的发展,利用区块链的数据不可篡改的特点,区块链上的智能合约越来越受到关注<sup>[15]</sup>。智能合约允许在不需要强制执行机制、可信任的第三方或法律系统的情况下,在未知方之间进行可信任的协议和交易。这种反差使得交易变得透明、可追踪和不可逆转。它们使得以无冲突和明确的方式交换资产、货币、财产或任何其他价

值成为可能,而不会招致第三方的费用,第三方由可自动执行的合同代码代替。

当满足智能合约的条件时,合约将自动执行相应的代码<sup>[16]</sup>。例如,执行转账功能的智能合约首先确定是否满足其激活条件;如果满足,则进一步验证相应交易是否可执行,包括交易是否被篡改,支出账户金额是否为零、足够等等。验证后,合同自动执行相应的交易。

## 2 CEPM-Chain 设计

文中提出的基于区块链技术的土建工程项目管理平台 CEPM-Chain 是一种基于区块链技术的土建工程项目流程管理及合约记录系统,利用区块链技术的去中心化、去信任、信息透明、数据不可篡改可溯源等特性来降低因偷工减料、以次充好、造假数据、材料的验收和管理上未严格把关等原因造成的工程事故的发生率。该平台提供一个基于联盟链的分布式账本,来保存与土建工程项目相关的合约文件、数据信息、数字签名等,最大限度地进行多方监督与管控,减少容易被伪造和共谋的手动流程,并自动创建记录和将数字签名输入区块链。该平台可提高土建工程行业项目管理的流程效率,消除该行业目前存在的信任、透明度和核查问题,从而更好地规范土建工程市场。且该平台将采用节点角色分工、信誉度机制、随机话语权增加等方法减少区块链联盟链采用的 PBFT 拜占庭容错算法具有的可扩展性低、通信复杂度高的缺点,从而提高系统的效率和性能。

### 2.1 系统架构设计

基于区块链技术的土建工程项目管理平台 CEPM-Chain 的参与者将包括认证机构、建筑材料供应链中的各方、土木工程顾问和承包商、现场工程师、测量员、政府部门以及公众。分布式账本维护人员将积极尝试向区块链添加新的区块。当新的数据块成功添加到区块链时,将生成令牌,并且需要将数字签名(交易)添加到区块链系统中。

CEPM-Chain 平台架构如图1所示。

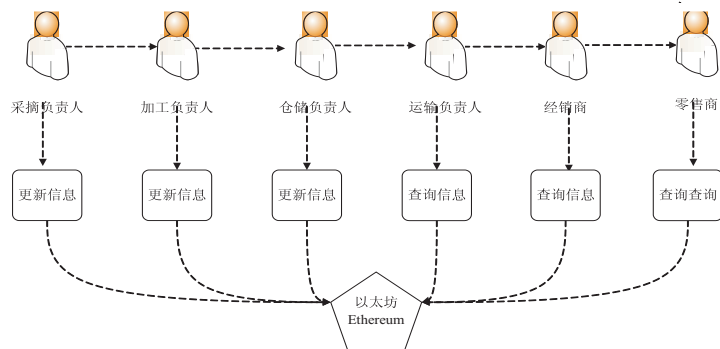


图1 平台参与者(角色)构成

CEPM-Chain 平台架构分五层,见图 2,自上向下 分别是:

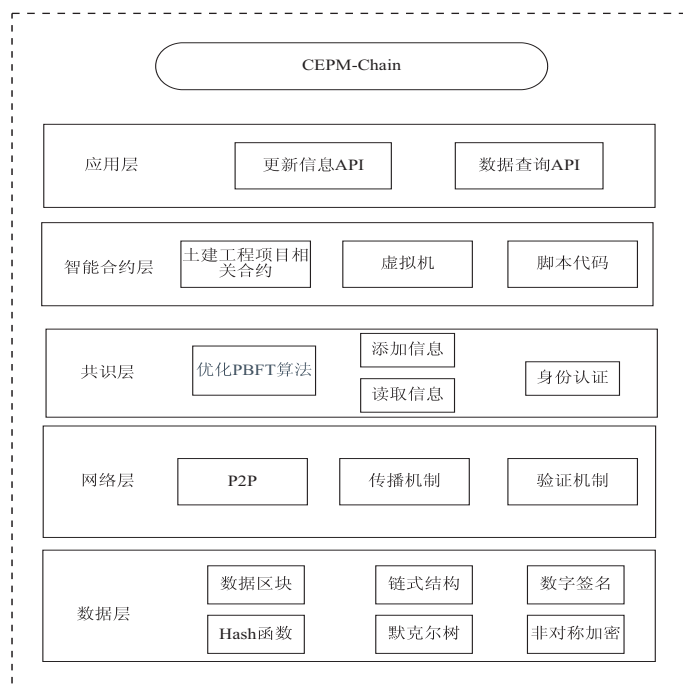


图 2 CEPM-Chain 架构

(1)应用层:CEPM-Chain 平台的用户(包括认证机构、建筑材料供应链中的各方、土木工程顾问和承包商、现场工程师、测量员、政府部门以及公众)通过应用层的 API 向 CEPM-Chain 平台添加信息或读取信息。

(2)智能合约层:该层包含三个模块,分别是以太坊虚拟机 EVM、脚本代码模块以及土建工程项目相关合约模块。以太坊虚拟机是以太坊运行智能合约的基础。其余两个模块可以将用户的信息以及他们在以太坊中产生的交易(例如,供货商添加原材料信息)都记录在区块链中。

(3)共识层:共识层基于 PBFT 算法为共识机制进行了优化设计,将在 2.2 节详细介绍。包括三个模块,分别为身份认证模块、添加信息模块以及读取信息模块。

(4)网络层:该层包含三个模块,分别是 P2P 网络、传播机制、验证机制模块。CEPM-Chain 平台是多类用户共同参与,并且在供应链中地位平等,因此 P2P 网络是 CEPM-Chain 平台的核心。

(5)数据层:数据层的数据区块存储基础数据,hash 函数、链式结构、默克尔树,可很好地保证数据的不可篡改性;基于非对称加密技术的数字签名可以避免假账以及冒充记账等情形的发生。

## 2.2 共识层优化设计

(1)所述系统是一条由一些工商部门注册在内的土建工程公司和监管部门共同维护并开放给所有土建工程项目参与者使用的联盟链。本系统对系统内的节

点进行分工,可减轻 PBFT 算法由于复杂度太高而导致的网络中节点个数多而无法实用的弊端。

将联盟链中节点分为区块认证共识节点(也充当信息整合从节点)、普通用户节点、信息整合主节点、信息整合备份主节点四种类型。如图 3,节点  $s_1$ 、 $s_2$ 、 $s_3$  和  $s_4$  代表本系统内区块认证共识节点,节点  $n_1$ 、 $n_2$ 、 $n_3$ 、 $n_4$ 、 $n_5$ 、 $n_6$  和  $n_7$  为普通用户节点。

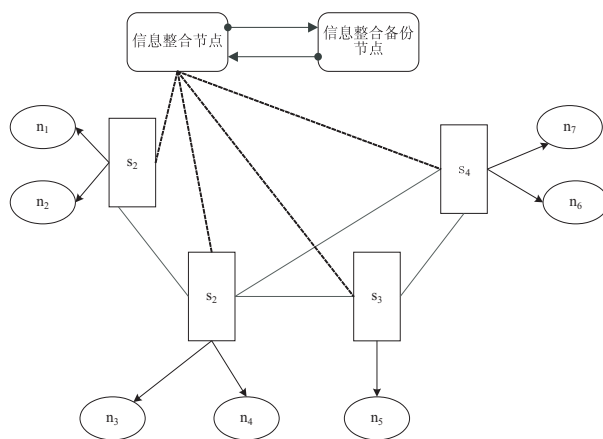


图 3 节点分类

### a. 区块认证共识节点。

区块认证共识节点是获得本联盟链授权的联盟参与者,该类节点之间构成全分布式结构,参与共识,认证区块的生成。同时区块认证共识节点也充当信息整合从节点。该节点将与普通用户节点间的交易信息及合约信息存储在本地磁盘上。

### b. 普通用户节点。

普通用户节点和所连接的区块认证共识节点及信



息整合主节点间形成客户端/服务器/服务器结构。普通用户节点作为客户端主要有两种功能,一是向其连接的区块认证共识节点发送资源查询请求,如果该区块认证共识节点没有发现所需资源,则向信息整合主节点转发请求,信息整合主节点找到相关信息的文件块和从节点间的映射关系,从有该信息的从节点中调取具体文件块信息转发给该区块认证共识节点继而将信息传给该普通用户节点。二是与其他节点之间交易签订合同。

c. 信息整合主节点。

信息整合主节点存储每个区块认证共识节点的所有信息的元数据,如合约文件名、合约文件目录结构、交易信息成时间、交易双方签署人、文件块和从节点间的映射关系等。

d. 信息整合备份主节点。

信息整合备份主节点是为了消除信息整合主节点失效对系统可用性带来的影响,使得在信息整合主节点失效时替代它。

(2)通过对共识节点采用信誉度机制进行话语权区分、随机部分节点话语权增加、剔除恶意节点等方法提高共识系统的稳定性。

a. 该系统内共识节点的数量与普通用户节点数量之间形成一定比例(例如:1:50),共识节点数量随着普通用户节点数量的增加而增加,共识节点数量的增减属于系统级别事务,普通用户节点发起更改变为共识节点的请求,需得到系统内超过 2/3 共识节点验证通过才可以成功。

b. 对所有共识节点构建信誉积分制度,信誉度越高共识时话语权越大,系统初始时所有共识节点有相同的投分权利,一定时间内信誉度不合格的共识节点将取消其共识的授权;每次共识时将随机对少部分共

识节点进行暂时话语权增加,可以防止系统内出现较多信誉度较高节点恶意破坏系统。当某段时间内部分共识节点积分过低,可取消其充当为共识节点的授权。

3 仿真实验

文中基于区块链开源框架 Hyperledger Fabric 搭建了底层区块链网络,使用 Fabric SDK 编写应用交互层客户端,实验环境配置为: Docker 17.09.0-ce, HyperledgerFabric v1.1,程序运行环境为 i7 八代处理器,16 GB 内存,Window10 操作系统,Java 运行环境 JRE (Java runtime environment)。

使用以太坊节点仿真器 Ganache,模拟一个由 12 个节点组成的以太坊网络。假设 12 个节点参与交易并竞争记账,每个节点都有投票权且可投 10 票,用随机函数模拟节点投票,选出 3 个节点作为代理节点。图 4 为以太坊网络示意图。

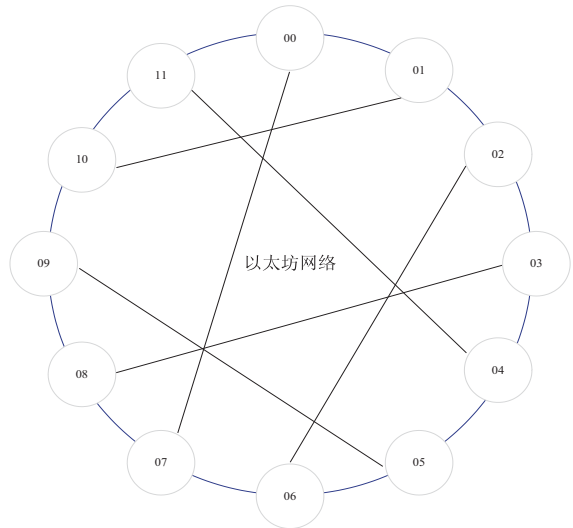


图 4 以太坊网络示意图

表 2 为以太坊节点仿真器生成的 12 个节点。

表 2 生成节点

节点	地址	用户
00	0x28F8C753352A7f6fC776dd01DEa70665c3b0e7aa	认证机构
01	0x6d1eA1E9ee2a62f20B5D996d3782fc408A352fCd	供应商
02	0x3893570c09FEBF99Ea515f8BA2e35A763e61dBA0	承包商
03	0xF36E95db6c7353f20B659bFa41cA474dC2B5BA26	承包商
04	0x3f7DFF5409eE3B56aBbF4E33973812C7E51a4082	政府
05	0x1552829F2C11eD36b670812C33f8370979664479	工程师
06	0x273F4a0F0a0799e3D9501bF8f47f9e8E39bfcFC7	认证机构
07	0xEDD0Bcfe5c6e5f5a4f2db8cE4b8902A8337A6105	供应商
08	0x83CcA876204C05d9440531C840769050919fd512	测量员
09	0x9cE2e4D22079D8248D4d127BC8983678BD0055f2	政府
10	0x0A979B707454a90d1Db78d30e85e4b21BE948080	测量员
11	0xd78819B3d7f983Cd15Ff8BB319Fdf4cE20350583	工程师

某次交易花费的时间主要取决于选取代理节点的用时,即“共识的时间”。40 次共识程序用时如图 5 所

示,最短用时 0.93 s,最长用时 1.05 s,有效提高了交易效率,使其在具体交易中有实用价值。

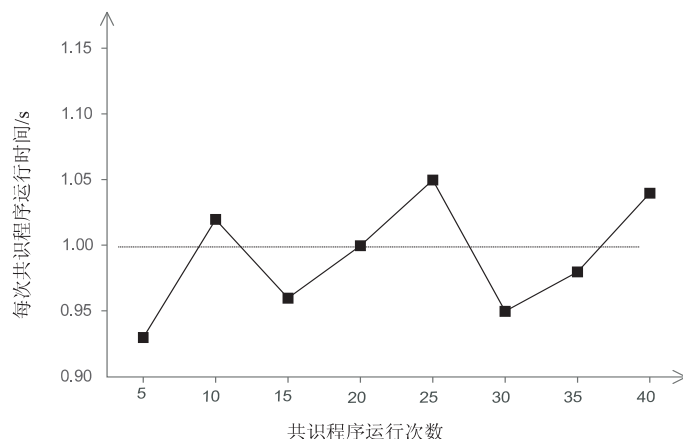


图 5 40 次共识程序运行次数统计

## 4 结束语

针对当前土建工程项目管理的痛点,文中提出了一种基于联盟区块链的土建工程项目管理平台 CEPM-Chain,探索了智能合约应用以及将该技术与土建工程信息建模和信息管理相结合的可行性。笔者认为区块链技术可以提高土建工程行业项目管理的流程效率,并消除该行业目前存在的信任、透明度和核查问题;同时采用节点角色分工、信誉度机制、随机话语权增加等方法解决区块链联盟链采用 PBFT 算法为共识机制的通信复杂度过高,可拓展性较低的弊端。该系统虽然在理论上具有一定的研究价值和优势,但要应用于现实场景之中,还存在诸多不足,需要进一步完善。

### 参考文献:

- [1] 李娜. 论如何实现土建工程管理的现代化[J]. 科技创新与应用, 2020(25): 191-192.
- [2] LAM R C Y, JUNUS A, MAK J Y W, et al. Blockchain for civil engineering practices in smart cities[C]//2018 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). Halifax, NS, Canada: IEEE, 2018: 1294-1300.
- [3] HARGADEN V, PAPAKOSTAS N, NEWELL A, et al. The role of blockchain technologies in construction engineering project management[C]//2019 IEEE international conference on engineering, technology and innovation (ICE/IT-MC). Valbonne Sophia-Antipolis, France: IEEE, 2019: 1-6.
- [4] 李长山. 土建工程管理创新及绿色施工管理方法探析[J]. 建材与装饰, 2020(2): 174-175.
- [5] XIONG F, XIAO R, REN W, et al. A key protection scheme

based on secret sharing for blockchain-based construction supply chain system[J]. IEEE Access, 2019, 7: 126773-126786.

- [6] 张仲华, 王静怡, 张孙雯, 等. 区块链技术在建筑工程领域中的应用研究[J]. 施工技术, 2020, 49(6): 1-5.
- [7] 李伟, 许志骋, 张彩芳. 区块链在金融行业的应用和发展[J]. 金融科技时代, 2020(2): 14-27.
- [8] 姚忠将, 葛敬国. 关于区块链原理及应用的综述[J]. 科研信息化技术与应用, 2017, 8(2): 3-17.
- [9] 刘彬. 我国“区块链+政务”发展现状及对策研究[J]. 现代营销: 下旬刊, 2020(12): 24-25.
- [10] 刘静. 区块链视角下企业业财融合与财务共享研究[J]. 现代商贸工业, 2021, 42(9): 105-106.
- [11] ZHAI X, ZHANG C. A cash flow blockchain based privacy-preserving[C]//2018 5th IEEE international conference on cloud computing and intelligence systems (CCIS). Nanjing, China: IEEE, 2018: 809-813.
- [12] 郭上铜, 王瑞锦, 张凤荔. 区块链技术原理与应用综述[J]. 计算机科学, 2021, 48(2): 271-281.
- [13] LI W, GUO H, NEJAD M, et al. Privacy-preserving traffic management: a blockchain and zero-knowledge proof inspired approach[J]. IEEE Access, 2020, 8: 181733-181743.
- [14] CHENG Y, HU X, ZHANG J. An improved scheme of proof-of-stake consensus mechanism[C]//2019 4th international conference on mechanical, control and computer engineering (ICMCCE). Hohhot, China: IEEE, 2019: 8260-8263.
- [15] 张志威, 王国仁, 徐建良, 等. 区块链的数据管理技术综述[J]. 软件学报, 2020, 31(9): 2903-2925.
- [16] WAN L, EYERS D, ZHANG H. Evaluating the impact of network latency on the safety of blockchain transactions[C]//2019 IEEE international conference on blockchain (Blockchain). Atlanta, GA, USA: IEEE, 2019: 194-201.