基于区块链和智能合约的财务管理系统建设

于爱荣[1],王 俊[2*],孙 海[3],王 勇[1]
(1. 中国人民解放军陆军工程大学 指挥控制工程学院,江苏 南京 210007;
2. 南京信息工程大学 管理工程学院,江苏 南京 210044;
3. 易霸科技(威海)股份有限公司,山东 威海 264200)

摘 要:财务管理是企业信息化建设中的一个核心环节,也是企业进行人力资源管理、业务流程控制与资金风险预判的重要依据。区块链技术的出现为企业进行财务管理系统的设计和改进提供了一种全新的设计思路,利用区块链技术本身所具有的去中心化和不可篡改的特性,可以保证企业财务管理系统中各类成本、支出、决算等数据的安全性和真实性。该文以区块链技术中的智能合约在中铁某企业财务管理系统中的应用为切入点,提出并设计了一种去中心化的系统设计方案,通过将智能合约与施工合同进行有机结合,确保只要施工合同进行交易,智能合约就能被即时触发,该机制从技术上确保了合同规定的权利与义务的严密执行,除此之外,智能合约还可扩展至多方交易,从而进一步简化传统多方交易面临的手续复杂等问题。同时,基于区块链技术上构建的多层次数据安全和追溯手段,也为企业的财务分析与决策提供技术支撑。

关键词:区块链;施工企业;财务管理;智能合约;软件设计
中图分类号:TP311 **文献标识码**:A **文章编号**:1673-629X(2021)04-0164-06
doi:10.3969/j.issn.1673-629X.2021.04.028

Financial Management System Construction Based on Blockchain and Smart Contract

YU Ai-rong[1], WANG Jun[2*], SUN Hai[3], WANG Yong[1]
(1. School of Command Control and Engineering, Army Engineering University, Nanjing 210007, China;
2. School of Management Science and Engineering, Nanjing University of Information Science & Technology, Nanjing 210044, China;
3. Yiba Technology (Weihai) Co., Ltd., Weihai 264200, China)

Abstract: Financial management is the core of enterprise information construction, and also the important basis for human resource management, business process control and capital risk prediction. The emergence of blockchain technology provides a new design idea for the design and improvement of financial support system for enterprises. By utilizing the de-centralization and non-tampering characteristics of block chain technology itself, the authenticity of all kinds of cost, expenditure, final accounts and other data in enterprise financial management system can be guaranteed. Based on the application of smart contract in the financial management system of an enterprise of China Railway, we propose and design a decentralized system design scheme. Through the organic combination of smart contract and construction contract, we can ensure that as long as the construction contract is traded, the smart contract can be triggered immediately, ensuring the strict implementation of the rights and obligations stipulated in the contract. Not only that, the smart contract can also be extended to multi-party transactions, so as to further simplify the complex procedures faced by traditional multi-party transactions. At the same time, the multi-level data security and traceability means based on blockchain technology also provide technical support for financial analysis and decision-making of enterprises.

Key words: blockchain; construction enterprise; financial management; smart contract; software design

收稿日期:2020-03-10 **修回日期**:2020-07-13
基金项目:江苏省重点研发计划(BE2018754)
作者简介:于爱荣(1979-),女,硕研,讲师,研究方向为区块链、大数据和复杂系统架构;通讯作者:王 俊(1979-),男,硕研,副教授,研究方向为人工智能、区块链。

0　引　言

近年来,作为新兴信息技术代表之一的区块链技术越来越受到了政府、企业和各类机构的广泛关注,并已经在许多领域得到了广泛运用。区块链是一种计算机技术的新型运用模式,其涵盖了分布式数据储存、P2P 技术、数据可信加密、共识机制等技术,究其本质来说,区块链就是一个个数据块的序列组合,在数据块上保存了交易信息的全部痕迹。区块链技术是一种新形态的分布式基础架构与计算范式[1]。

随着互联网技术的高度渗透,各企业的财务管理逐步从单机、局域网管理模式转变为云计算、移动网络化的新型管理模式。“十三五”期间,中国中铁各公司内部也构建了自己的财务管理系统,涵盖了公司内部管理所涉及到的人员、物资、材料、机械等多类资源,这些系统往往依托于互联网开发。虽然系统的建设极大地便利了企业的财务管理工作,提供比较准确的查询与分析等服务,为企业决策者和业务管理部门提供了财务情况查询的可信数据来源,但是,由于大部分信息系统在设计时采用数据库集中设计、存储和管理的模式,随着系统建成和上线运行,系统管控数据的中心化特征逐步凸显,数据中心化导致的数据易于被攻击、被篡改的风险隐患逐渐加大,特别是在财务管理中,一旦出现数据安全问题,将会对企业的正常业务管理造成不可预估的恶劣影响。财务信息系统以上所暴露的问题,其本质是由于系统设计架构的“过于中心化”,数据与管理的集中是该系统的最主要特征。而伴随着区块链技术的出现,为这类构建在集中数据管控业务系统所面临的数据中心化存储、信息易被篡改等问题,提供了一种有效的技术解决思路[2-3]。

该文引入区块链和智能合约技术,将区块链技术的去中心化和安全性的特性应用到了企业财务管理中,使得企业的财务及相关原始凭证数据的安全性和真实性得到了保障,而且对企业内部下属的分支业务管理节点达成共识,每个分支业务节点都将是维护系统、存储数据的组成部分,从而降低数据的管理维护的成本。通过系统构建的区块链网络,每一次数据(包含财务数据和业务数据)的改动都会永久地记录在链中,同时,链上的所有信息全部公开,全程可追溯,确保数据的真实[4]。

1　区块链与智能合约

1.1　区块链技术

区块链是目前最炙手可热的新兴计算机技术之一,其概念最先来源于 2008 年中本聪发表的《比特币:一种点对点的电子现金系统》一文。在该文中,作者描述了一种去中心化的电子先寄给系统的架构思想,该架构建立在 P2P 网络、数据加密算法和时间戳技术之上。比特币(Bitcoin)是区块链技术应用的最典型和最成功的案例。通过区块链技术,网络上的任何个体在无第三方可信机构参与的条件下,能够自由交易,同时保证交易全过程的匿名和可追溯[5-6]。

如今,区块链技术应用范围不断延伸,逐渐从以往的加密数字货币演变为一种提供可信区块链即服务的平台,区块链技术对传媒、医疗、物管、财会等多个传统行业的影响日趋加深,人们也在积极探索“区块链+”的行业应用创新模式。一般说来,区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成[7-8]。具体如图 1 所示。

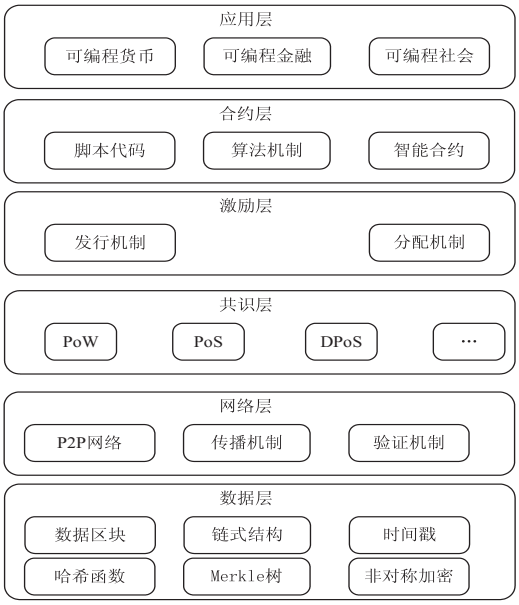

图 1　区块链基础架构模型

其中,数据层和网络层分别提供了数据加解密算法和网络分发与传播机制;共识层通过各类共识算法来解决分布式系统的一致性问题;激励层主要包括经济激励的发行机制和分配机制等;合约层是建立在整个区块链虚拟机之上的规则和商业逻辑,包含各类的算法、脚本和合约规则等;应用层则提供了各类典型场景和范例[9-11]。

1.2　智能合约

智能合约(smart contract)是指一种特殊的计算机协议,该协议无需人为干预,一旦被制定和部署之后即可实现自我执行和验证。通过智能合约不仅可以实现去中心化的流程化操作,而且交易安全、公平和全程可追踪。有的文献中将智能合约描述为“执行合约条款的计算机交易协议”[12]。

1.3　区块链和智能合约的优势

智能合约的出现有效解决了传统人与人制定合约中存在的双方信任问题。通过使用区块链技术,充分利用智能合约在合约规则制定、执行等方面的优势,避

免主观恶意行为对合约的干扰。通过在区块链上部署智能合约,确保了在链上合约可以公平、公开、透明和可追溯的执行下去[13]。

1.3.1 合约的精准执行

由于智能合约部署前对合约中的执行条件、交易规则和交易过程节点做出了明确界定,一旦合约在数据链上进行部署,计算机即可按照合约规定步骤进行执行,合约执行的结果都将精确记录,不会出现合约预期外的执行分支和结果[14]。

1.3.2 较低的人为干预

智能合约部署在区块链之后,合约的所有条款和执行结果都无法进行修改,避免了现实合同中存在的人为操纵和干预的可能,确保合约各方公平执行合约。

1.3.3 可信的合约管理

智能合约的执行无需可信任的第三方机构或中心进行参与,也就是说,智能合约的全过程管理无需第三方的权威机构来对合约是否按规定执行进行认证,同时,合约执行过程中的监督和分歧仲裁也由计算机系统自行来完成[15]。

1.3.4 廉价的合约成本

智能合约具有自我治理、无需人为干预的智能化特征,当智能合约部署完成之后,在合约的条件触发、流程执行、分歧处理等以往需要人为干预的环节可以进行程序化处理,实现近乎零成本的人力资源投入。但要达到全程无需人为干预的目标,需要智能合约参与方能够将合约的每个细节都要考虑清楚,并在合约部署前确定下来[16]。

2 区块链与财务管理系统的结合

2.1 区块链与工程管理的结合

施工企业在开展建设过程中面对的各个合作供应商、材料和设备时,最关心的是质量,同时施工全过程的质量控制也是企业关注的核心。施工涉及到的质量管理涵盖了对施工项目的材料、人员、设备、工序等各个方面的规范性要求。由于区块链技术具有来源可追溯的特性,充分利用该特点,将质量过程中的各个节点进行记录,从而可精准查询不合格工序的问题,责任是由谁来承担,哪家生产单位的建筑材料有缺陷的等等。区块链技术的运用为工程质量的实时监督和事后追责提供了可能,同时也有利于材料供应链管理、工程设备租赁、材料自动采购和支付、预制品出厂前和出厂后溯源性管理[17]。

2.2 区块链与施工成本控制

施工成本主要由人工费、材料费、机械使用费、管理费、税金等多方面组成,每一笔费用的支出和进入都需要进行成本控制。利用区块链对交易的记录,可实现现场施工成本的分析与预警,并可将问题实时反馈到某项施工专业和施工活动中去,即时对管理人员进行提醒。同时区块链技术的加密算法对工程敏感数据可进行隐私保护,对核心敏感的工程项目的人工费、材料费、机械使用费等数据信息进行脱敏处理后,在保护项目隐私的情况下提供安全的分布式数据存储方案[11]。

2.3 区块链与施工合同管理

区块链中的智能合约与施工合同的形式类似,在设计合同管理时充分基于智能合约技术。具体内容包括:

(1)构建自动执行的智能合约合同条款,解决合同上存在的拖延、扯皮等不严谨问题。实现了合同当事人无须信任彼此,无须建立在对任何个体、法律规则或社会机构的信任之上。

(2)将施工合同在智能合约的体系框架下数字化,使得能够利用计算机快速、准确地查阅和研究,能够避免出现伪造合同、阴阳合同的出现,有利于合同的动态管理和有效监管。

(3)采用智能合约大大降低了合同签订、履行和监管方面的人力与资源成本消耗,并且为合同履行过程中的索赔提供技术手段。

2.4 区块链与施工信息管理

施工信息管理主要包括施工过程中产生的大量票据、文件、人员、财务信息等各类过程性数据,以往这些数据停留在系统外,通常无法采集和利用,利用区块链技术可在链上的任何节点进行采集和存储,方便各项施工数据管理。将数据进行充分处理和整合之后,有利于施工企业在各管理领域如成本,质量、安全等管理水平的提高,数据的流通和整合将有利于促进企业管理水平的提升。

3 基于区块链的财务管理系统设计

3.1 系统运行架构

基于区块链和智能合约的财务管理系统主要由财务支撑服务平台和项目部管理系统两部分组成,见图 2。财务支撑服务平台提供基于区块链和智能合约的工程、合约、机械、财务等多维信息的管理,并对共享数据的行为进行激励,促进平台的活跃和成长[18]。项目部管理系统基于大数据和人工智能技术,构建适合工程项目部实际的施工业务分析、管控、预警等模型、算法和管理流程,项目部管理系统还可将相关的模型和算法实现为智能合约,上传到财务支撑服务平台中,也可以从平台中下载所需的智能合约,系统的运行架构如图 2 所示。

以区块链技术为核心的财务支撑服务平台提供了

可信赖的区块链运行环境,为区块链上运行的各工程项目部管理系统提供基础支撑,同时,服务平台将区块链技术进行技术封装和业务整合,方便其到工程项目部中的集成使用。运用区块链技术的工程管理包括合约、工程、机械、物资管理等各个环节。平台通过以开放自定义化智能合约的方式帮助各项目部实现自主的成本分析和质量控制,从而降低施工企业项目实施过程中使用区块链技术的门槛,通过利用区块链技术的可信度高、防篡改等特性,有效解决施工管理中的监管难、取证难等问题,有效提升施工企业的科学管理运营水平。在本架构中,整个服务平台对运算资源和存储资源均实现了虚拟化,同时,采用公私密钥体系来对数据进行安全控制,确保数据存储和管理的安全可控。

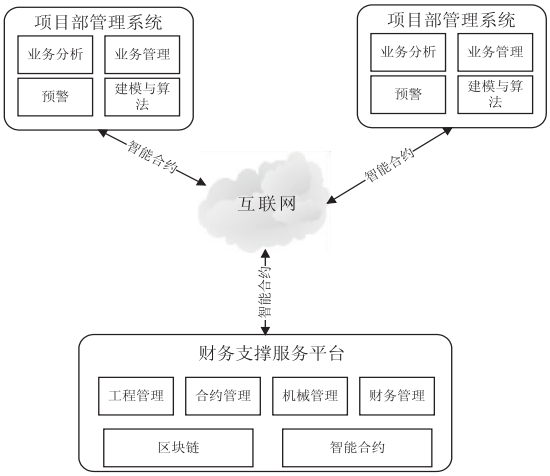

图 2　系统运行架构

3.2　财务支撑服务平台的技术架构

财务支撑平台采用分层设计的技术思路,自下而上划分为基础设施层、数据层、服务支撑层、业务应用层和系统接入层五部分,技术架构如图 3 所示。

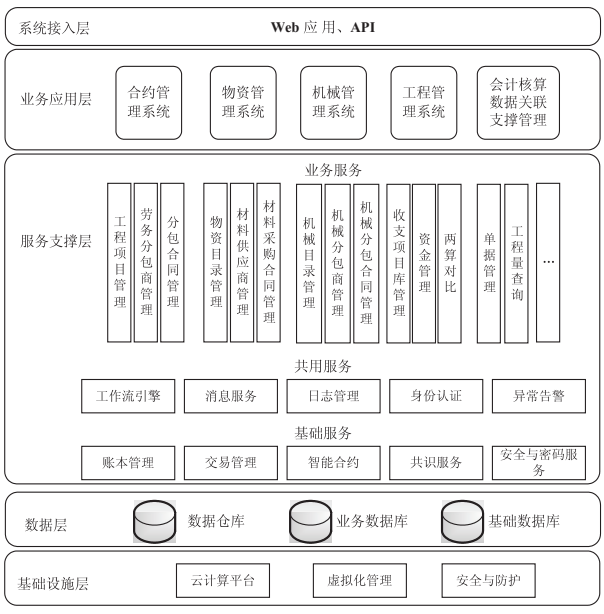

图 3　财务支撑服务平台的技术架构

3.2.1　基础设施层

提供平台运行所需的云计算与虚拟化环境,涵盖平台所需的操作系统、系统软件等基础设施。

3.2.2　数据层

为工程、合约、物资等业务系统提供数据集成、存储的基础平台,形成统一的基础数据、字典数据、业务数据和交互共享的集成数据,为数据高效分析和综合利用奠定基础。

3.2.3　服务支撑层

为决策部门和业务管理部门提供全面的数据分析处理和面向业务应用的数据服务。基础服务包括账本管理、交易管理、智能合约管理等;共用服务包括工作流引擎、消息服务、日志管理等;业务服务涵盖了合约、物资、机械等各业务处理。

3.2.4　业务应用层

在服务支撑层提供各类服务的基础上,提供了流程化的管理功能,每一个业务应用模块均可以独立运行或组合应用。同时提供二次开发接口便于无缝集成。

3.2.5　系统接入层

为项目部管理系统提供内网或外网的接入服务,形式涵盖网站、程序客户端和移动 APP 等。

4　智能合约的架构分析

4.1　智能合约的定义与特征

智能合约概念的提出已有很长时间,通常将智能合约定义为一种“执行合约条款的可计算交易协议”[19]。从狭义上来说,智能合约是包含商业活动逻辑、规则和算法的程序代码,可将行为人、权责义务和相互关系程序化。从广义上来说,智能合约是一种特殊的计算机协议,一旦生效后能实现自我执行、验证和自治。智能合约不仅仅可运用于金融领域,其在物联网、数字版权、公共服务等领域都有很广阔的前景。智能合约在使用时类似于普通合约,其生命周期包括生成、发布和执行三个阶段,具体如图 4 所示。

合约生成阶段主要包括了合约参与方协商、合约定义与规范、合约验证以及合约代码生成四个环节。通过合约参与方的沟通协商可明确合约参与个体的责任、权利、义务和利益等,确定形式化的合约文本并实现其标准化和程序化,经过验证后可以生成规范的合约代码。在合约标准化和验证环节中需要引入特定领域的知识专家一起进行商定和研究,验证过程应科学、合理和可追溯,确保合约文本与合约代码的一致。

合约发布阶段通过 P2P 方式将合约代码分发至每一个区块节点,区块节点对收到的合约存储并进行在线共识。共识的过程中需要对合约进行 HASH 计

算和比对,经过多次比对后形成对合约的共识,并以区块方式进行全网的扩散。

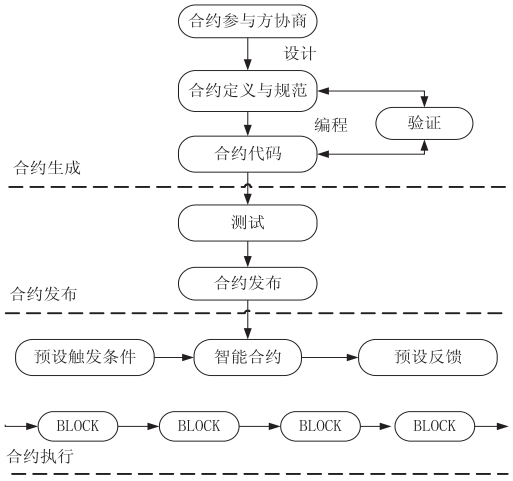

图 4 智能合约的生命周期

合约执行阶段严格按照“事件触发”机制,一旦合约预设的触发条件达到,将会把合约排入等待验证的队列,待验证的合约会推送至区块上的每一个节点,验证通过的合约经过共识后便会成功执行。整个合约的处理过程都由区块链底层内置的智能合约系统自动完成,公开透明。不可篡改同时结果进行及时反馈。

4.2 智能合约的架构

智能合约的架构如图 5 所示。自下而上划分为数据层、传输层、智能合约对象层、验证层、执行层和应用层 6 个部分。

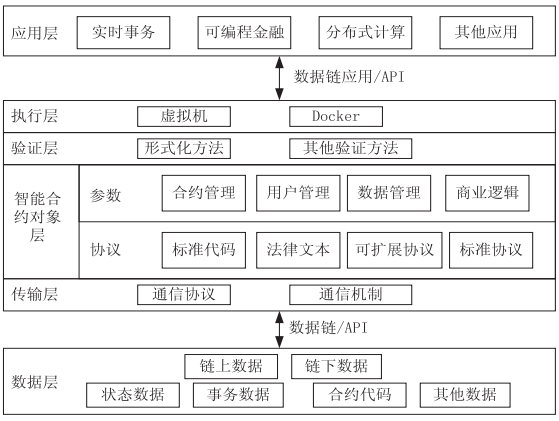

图 5 智能合约的基本架构

其中,数据层包括了链上和链下数据,为上层提供必要的数据源;传输层为数据交互提供协议和机制保证;智能合约对象层提供参数和协议两部分的管理;验证层主要以形式化方法对合约代码进行判定,确保和合约文本保持一致;执行层只要提供了智能合约运行的基础软件环境;应用层提供面向业务支撑的应用,涵盖分布式计算、事务处理、可编程金融等。

5 智能合约的施工合同管理

智能合约在区块链技术中的定位类似于现实生活中的合同或协议,所有在链上的参与者都需要遵照智能合约的约定规则来完成特定的行为或交易。设计者通过编写和完善智能合约内容规定用户行为、交易准则和交易步骤等细则。智能合约完成后需部署在区块链网络中,部署后的智能合约对用户是不可见的,这一特性也保证了智能合约的隐秘性。施工合同作为财务管理中的重要环节,合同执行是否安全性和公平性的问题,一直以来都是企业管理中难于处理的课题。通过引入智能合约,只要开始进行交易,智能合约就能够被即时触发,保证了规定的权利与义务的严密执行,同时智能合约不仅能被用于双方交易,还能被用于多方交易,简化了传统多方交易面临的手续复杂等问题[20-21]。

5.1 智能合约的形式化定义

合同通常由一系列的关联约定构成,约定描述了一方需要承担的义务。约定是合同组成的基本单位,在智能合约中该文对约定进行了如下定义:

约定是一个五元组 A(a,b,c,o,tl),含义是乙方 a 向甲方 b 做出承诺,如果条件 c 达成,就产生操作。其中:

(1)条件 c 值是布尔型。当为 true 时,表示条件成立,而为 false 时,表示条件未成立;

(2)tl 表示该约定的时间周期,tl 为 true 时该约定有效。

约定在其时间周期内有不同的状态[22-24],状态的变化如图 6 所示。

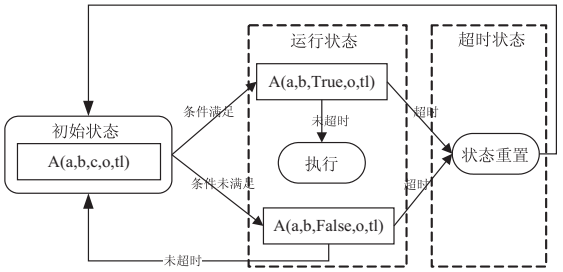

图 6 智能合约的状态转换图

5.2 智能合约的代码实现

智能合约是一个状态机,因此必然包含状态机和一系列接口函数,本系统的智能合约开发用 solidity 编程语言,下面以机械合同交易为例,展示核心代码[25]。

```
contract Purchase_Mechanics {
    uint public Price;//价格
    address public sellman;//卖方
    address public buyman;//买方
enum State {Created,Locked,overtime,over}
    State public state;  //当前状态
…
//修饰符,确保是卖方
modifier onlySellman () {    …    }
```

```
//修饰符,确保是买方
modifier onlybuyman ( ) {      …      }
//交易部分
function confirmPurchase( )
public
inState( State. Created)
//判定交易成立的条件
condition( msg. value = = (150000) )
payable
    {
emit PurchaseConfirmed( ) ;
buyman = msg. sender;
state = State. Locked;
    }
//买方确认收到机械实体,解锁 ether
function confirmReceived( )
public
onlyBuyman
inState( State. Locked)
    {emit ItemReceived( ) ;
        //需要提前设置状态为结束
state = State. over;
buyman. transfer( value) ;
sellman. transfer( this. balance) ;
    }
```

6　结束语

该文在充分研究区块链和智能合约技术的基础上,针对目前企业传统财务管理中存在的对各类成本、支出、决算难于精准可信掌握的难题,设计并实现了一种基于区块链的系统构建方案,将智能合约与施工合同进行了有机结合,完成了合同的形式化表示和合同交易的代码实现,对区块链技术在施工企业财务管理工作中的应用进行了初步探索。

参考文献:

[1] 王璞巍,杨航天,孟　佶,等. 面向合同的智能合约的形式化定义及参考实现[J]. 软件学报,2019,30(9):2608-2619.

[2] 朱雅菊. 区块链技术在建筑行业的应用场景展望[J]. 工程经济,2018,28(6):45-47.

[3] 李中振,高超越,刘　敏,等. 基于区块链技术的学籍管理系统[J]. 四川大学学报:自然科学版,2019,56(3):450-456.

[4] NAKAMOTO S. Bitcoin:a peer-to-peer electronic cash system[EB/OL]. 2018-12-23. https://bitcoin. org/bitcoin. pdf.

[5] 蔡维德,郁　莲,王　荣,等. 基于区块链的应用系统开发方法研究[J]. 软件学报,2017,28(6):1474-1487.

[6] KOSBA A, MILLER A, SHI E, et al. Hawk:the blockchain model of cryptography and privacy-preserving smart contracts[C]//Security and privacy. [s. l.]:IEEE,2016.

[7] 李文森,王少杰,伍旭川,等. 数字货币可以履行货币职能吗?[J]. 新理财,2017(6):25-28.

[8] 张　健. 区块链:定义未来金融与经济新格局[M]. 北京:机械工业出版社,2016:38-40.

[9] 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.

[10] 阿迪瓦特·德什潘德,凯瑟琳·斯图尔特,路易斯·列皮特,等. 理解分布式账本技术/区块链—挑战、机遇和未来标准[J]. 信息安全与通信保密,2017(12):20-29.

[11] SZABO N. Smart contracts[EB/OL]. 2018-11-05. http://www. fon. hum. uva. nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo. best. vwh. net/smart. contracts. html.

[12] STARK J. Making sense of blockchain smart con-tracts[EB/OL]. 2018-11-05. https://www. coindesk. com/making-sense-smart-contracts/.

[13] 张　波. 国外区块链技术的运用情况及相关启示[J]. 金融科技时代,2016(5):35-38.

[14] 乔海曙,谢姗珊. 区块链金融理论研究的最新进展[J]. 金融理论与实践,2017(3):75-79.

[15] WOOD G. Ethereum:a secure decentralized generalized transaction ledger (EIP-150 revision)[EB/OL]. 2018-11-05. http://gavwood. com/paper. pdf.

[16] 曹文岩,李明柱,王　婉,等. 区块链与施工管理相结合的应用展望[J]. 现代商贸工业,2019,40(18):91-92.

[17] 黄宇翔,梁志宏,王跃华,等. 区块链在供应链金融中的应用研究[J]. 计算机科学与应用,2018,8(1):78-88.

[18] 周潇茜,刘丽华,任锦鸾,等. 区块链技术在数字媒体资产版权保护中的应用[J]. 服务科学和管理,2019,8(2):75-80.

[19] 蔡文军,朱　艳. 应用于能源系统的区块链技术研究进展[J]. 智能电网,2018,8(3):205-212.

[20] 谭　征. 区块链视角下物流供应链重构研究[J]. 商业经济研究,2019(5):83-86.

[21] 樊树伟. 基于区块链的数据访问控制方法及应用研究[J]. 数码世界,2019(7):2-3.

[22] 刘敖迪,杜学绘,王　娜,等. 基于区块链的大数据访问控制机制[J]. 软件学报,2019,30(9):2636-2654.

[23] 张亚伟,张问银,王九如,等. 基于区块链的数字资产管理系统框架设计与分析[J]. 计算机科学与应用,2019,9(1):28-37.

[24] YE P J, WANG S, WANG F Y. A general cognitive architecture for agent-based modeling in artificial societies[J]. IEEE Transactions on Computational Social Systems,2018,5(1):176-185.

[25] ATZEI N, BARTOLETTI M, CIMOLI T. A survey of attacks on ethereum smart contracts[C]//Proceedings of the international conference on principles of security and trust. Berlin, Heidelberg:Springer,2017:164-186.