doi:10.3969/j.issn.1672-4348.2019.01.012

基于区块链技术的数字资产确权交易模型研究

张婷

(福建工程学院 应用技术学院,福建 福州 350003)

摘要:针对传统数字资产版权登记、签权、授权、交易等问题,提出基于区块链技术的数字资产确权交易模型;研究并设计该模型的逻辑结构及模型中数字签名、版权注册、区块链智能合约等模块的流程设计;在模型关键模块流程设计的基础上,重点结合数字签名技术、区块链智能合约、非对称数字加密等技术和相关的算法,实现了基于区块链技术的数字资产确权交易模型。最后,通过实验验证了模型中数字签名身份验证及数字内容解密算法的安全性和相关性能。

关键词:区块链;数字资产;确权交易;智能合约

中图分类号:TP311.13 **文献标志码**:A **文章编号**:1672-4348(2019)01-0065-07

A study of digital assets' copyright confirmation and transaction based on block chain technology

ZHANG Ting

(School of Applied Technology, Fujian University of Technology, Fuzhou 350003, China)

Abstract: Aiming at the problems of copyright registration, signature, authorization and transaction of traditional digital assets, a model was put forward for the confirmation and transaction of the copyright of digital assets based on block chain technology.The logical structure of the model was studied as well as the process design of digital signature, copyright registration and smart contracts of the block chain in the model. On the basis of the process design of its key modules, the model for the confirmation and transaction of the right of digital assets based on block chain technology was realized by focusing on the combination of digital signature technology, block chain's smart contracts, asymmetric digital encryption and related algorithms. Finally, the security and related performance of the digital signature authentication and digital content decryption algorithm in the model were verified by experiments.

Keywords: block chain; digital assets; confirmation and transaction; smart contracts

当前,互联网发展从信息互联网迈入价值互联网阶段,数据资源成为国家核心战略资产和社会财富。然而数字空间的可扩展性、可复制性和多维可塑造性等特征在提供蕴藏海量财富可能性的同时也给网络侵权行为带来了极大的便利。网络侵权行为的广泛性和严重性也引起了政府的高度重视。《国民经济和社会发展第十三个五年规划纲要》对有效打击侵权,强化尊重原创、遵守法律和促进产业创新、保护产权等做出了明确具体的部署。2016 年 6 月,国务院在《促进科技成果转移转化行动方案》中强调为促进科技成果转化和技术转移,加快科技成果与资本的有效对接,应加强“互联网+”融合重点领域的知识产权服务,提升产业创新发展能力。2017 年 2 月,国家新闻

收稿日期:2018-11-02
基金项目:福建省教育厅中青年教师科技类项目(JAT170400)
作者简介:张婷(1984-),女,陕西宝鸡人,讲师,硕士,研究方向:计算机应用。

出版广电总局在印发的《版权工作“十三五”规划》突出强调网络领域版权监管,推进网络环境下确权、授权和交易规则等顶层设计,构建版权产业又好又快发展格局[1]。数字资产无法确定权利归属,也就无法进行交易,大数据产业的价值也就无法开发。因此,数字资产确权机制的研究不仅顺应政府决策,而且能够促进数字资产的良性交易,是一项既利当前又利长远的重要举措。

传统的版权保护方法都是集中登记式的,本质上是一种权威管理机构授权的中心化的版权管理机制,存在确权难、盗版严重、公开性差、维权成本高等问题。区块链具有防篡改、可信任、去中心化、分布式、可靠性等特点,对于价值互联网时代的物质和服务增值、数字资产增值、社会价值体系重构等具有巨大的潜力,越来越受到政府机关和科技组织的重视[2]。2016 年 10 月,工信部发布了《中国区块链技术和应用发展白皮书》,指出使用区块链技术,可以通过时间戳、哈希算法证明一段文字、视频、音频等存在性、真实性和唯一性。一旦在区块链上被确权,数字资产的后续交易都会被实时记录,并可追溯、可追踪,这也为司法取证提供了一种强大的技术保障和结论性证据[3]。

综上所述,中国面向大数据环境下的数字资产版权保护机制还处于探索阶段。本课题在分析数字资产权利属性以及其对数字化经济良性发展重要性的基础上,针对数字资产版权保护的特点,探讨新型保护技术,构建数字资产确权交易模型,为政府部门制定数字资产相关管理制度、政策等提供依据。将区块链理解为一项针对数据进行可信化处理的底层技术,探索其在数字资产版权保护领域的发展前景。

本课题针对目前数字资产版权确权、授权、交易等问题,提出并设计基于区块链的数字化版权资产确权交易模型,如图 1 所示。

该模型将数字资产的生命周期,分为登记、签权、交易、支付 4 个过程。资产的登记确权作为整个模型中相对前端的一环,它主要通过将数字资产的创作者信息、内容信息、创作时间信息以及初始传播信息通过加密解密算法换算和抽象,形成缩略数字信息,记录在区块链中,使得所有数字内容能够简单、快捷、低成本的完成原创版权登记。版权创建者与产品使用者,通过区块链智能合约进行版权购买赎回及购买支付,购买完成结果返回第三方。

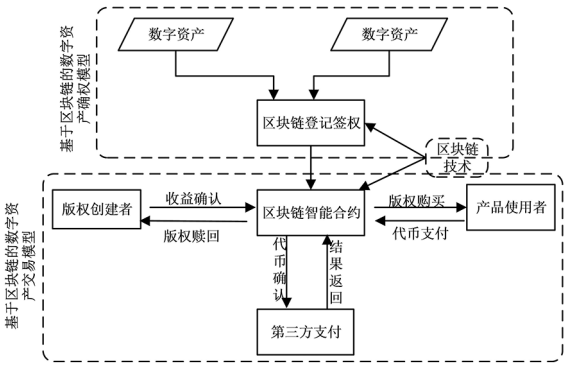

图 1 基于区块链技术的数字资产版权确权模型

Fig.1 Model of digital assets' copyrightconfirmation and transaction based on block chain technology

1 国内外研究现状

随着互联网技术不断发展和完善,在提升数字资产供应链价值的同时,也对数字资产版权保护问题提出了更高的要求。

1.1 现有的数字资产版权保护方法及其局限性

目前,在网络化时代,数字版权授权需求量激增,而现行的版权管理机制具有过程复杂、成本较高、效率较低等特点,已明显无法适应互联网时代数字版权贸易的要求。首先,传统的版权保护技术通常采用简单的加解密方式,而这种简单解密方式并不能实现对数字内容的全方面保护,具有一定的局限性。其次,传统的版权保护方法不仅不够精确、容易出错,而且没有严格可信的可追溯性,给调查取证带来许多问题。再者,传统的版权保护方法面临确权时效性、数据分散性及交易的不透明性,当使用者将数字产品加工后继续交易,后续使用者并不能明确作品的权利所属等问题,并且传统的版权保护都是集中登记式的,本质上是一种权威管理机构授权的中心化的版权管理机制,存在确权难、盗版严重、公开性差、维权成本高等问题[4]。

1.2 区块链技术应用现状研究

2008 年,随着比特币的发行及其创立者中本聪的论文《比特币:一个 P2P 电子现金系统》的发表,区块链作为比特币系统的底层核心技术开始进入人们的视野。区块链技术的应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域[5]。

区块链是由区块有序链接起来形成的一种数据结构，其中区块是指数据的集合，相关信息和记录都包括在里面，是形成区块链的基本单元，每个区块由区块头和区块主体组成[6]。一般而言，区块链技术包含分布式账本技术、共识机制技术、智能合约技术和密码学技术。分布式账本技术本质上是一种可以在多个网络节点、物理地址 或组织构成的网络中进行数据分享、同步和复制的去中心化数据存储技术。共识机制是指多方参与的节点在预设规则下，通过多个节点交互对数据、行为或流程达成一致的过程，其中共识算法是关键。密码学技术是信息技术的基石，在区块链中，信息的传播按照公私钥这种非对称数字加密技术来实现交易双方的互相信任[7]。

2　基于区块链技术的数字资产确权交易模型设计

2.1　模型的逻辑层设计

图 1 确权交易模型中，将数字资产的生命周期，分为登记、签权、交易、支付 4 个过程；其中，区块链签权与区块链智能合约是核心业务。该模型的逻辑层分为大数据基础设施、区块链端、服务端、应用端、交易端、监管端。应用端主要完成用户及资产的登记与注册、版权授权及分发控制；交易层完成版权的购买及赎回、收益确认及支付；服务端完成资产及权限管理、用户及资产信息的隐私保护；大数据基础设施主要完成数据主体确权、数据存储、区块链数据云存储服务、监管端完成应用端监控、模型池监控、数据源监控、交易规则监管等[8]。模型的逻辑层设计如图 2 所示。

2.2　区块链登记签权

数字资产的登记确权作为整个模型中相对前端的一环，它主要通过将数字资产的创作者信息、内容信息、创作时间信息以及初始传播信息通过加密解密算法换算和抽象，形成时间戳的缩略数字信息，记录在区块链中，使得所有数字内容能够简单、快捷、低成本的完成原创版权登记[9]。区块链登记确权这一核心业务主要包含给用户签发数字证书、给数字资产添加水印、生成时间戳保存在区块链中 3 个关键环节。由于区块链是由区块有序链接起来形成的一种数据结构，区块是形成区块链的基本单元，每个区块由区块头和区块主体组成。故此，区块链的每个区块头中将保存的是资产的时间戳缩略信息，后期各个资产的识别是通过它的时间戳缩略信息进行识别的[10]。

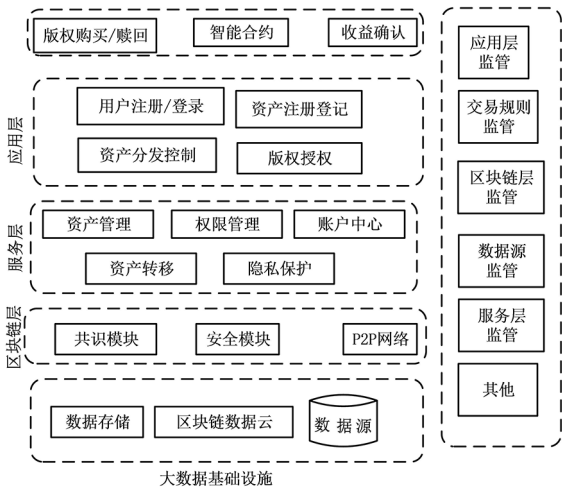

图 2　模型的逻辑层设计

Fig.2　Design of the model's logic levels

2.2.1　用户数字证书的签发

在数字证书的签发流程中，用户通过模型应用端进行登录和注册，并在系统中发出申请证书的请求；数字证书认证中心向密钥管理中心请求加密密钥、签名密钥及签名验证算法；密钥管理中心生成加密密钥；认证中心对用户信息进行签名生成证书。数字证书的签发如图 3 所示。

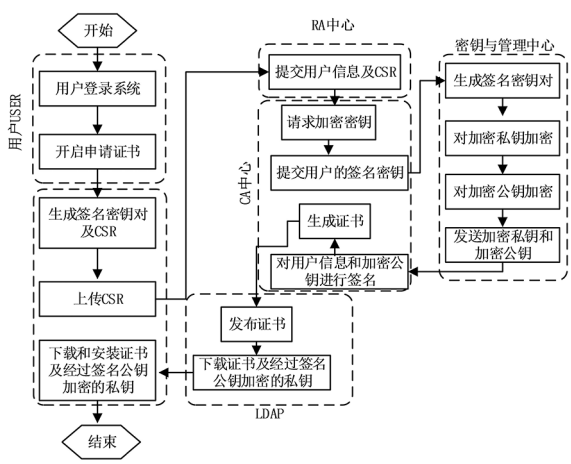

图 3　数字证书签发流程

Fig.3　Digital certificate's issuing process

2.2.2　生成时间戳缩略数字信息

资产版权注册的过程中最终输出的是时间戳缩略数字信息，核心业务包含给资产内容添加水印信息和生成时间戳缩略数字信息两个部分。主

要分为以下 5 个主要环节:(1)用户下载并安装自己的数字签名证书和经过签名公钥加密的私钥;(2)用户先对资产进行水印信息的添加之后,再向数字内容提供商提交数字资产并获取签名;(3)版权控制服务器验证签名信息并解密;(4)版权控制服务器向密钥管理与认证中心中申请时间戳缩略数字信息;(5)密钥管理与认证中心向版权控制服务器返回时间戳缩略数字信息,并保存时间戳信息到区块链的区块头中。具体流程如图 4 所示。

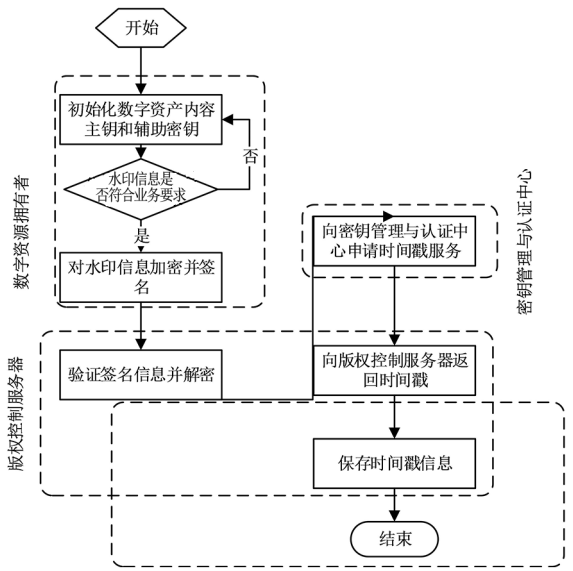

图 4 版权注册流程

Fig.4 Copyright registration process

2.3 区块链智能合约

在本文提出的数字资产确权交易模型中,确权业务完成后生成的时间戳缩略数字信息保存在区块链中。而版权创建者与产品使用者两者之间是通过区块链智能合约进行版权购买赎回及购买支付,购买完成结果返回第三方。

模型中的区块链智能合约实质是控制区块链网络中的版权创建者与产品使用者之间对数字资产按照交易规则进行编码,能够自动执行且可以部署在以太坊网络上运行的一段代码[11]。

模型中的区块链智能合约是资产版权交易核心业务,分为版权创建者与产品使用者之间业务、第三方机构之间业务和汇率表查询业务。版权创建者通过区块链合约进行版权赎回和收益确认;产品使用者通过区块链合约进行版权购买和版权费用支付;第三方机构间业务主要进行资产汇率表的建立、更新和跨机构交易等。在区块链智能合约执行交易之前,模型中需要根据区块链登记确权过程中给用户生成的数字签名进行版权交易双方的身份确认之后再进行版权交易[12]。模型中智能合约的执行原理如图 5 所示。

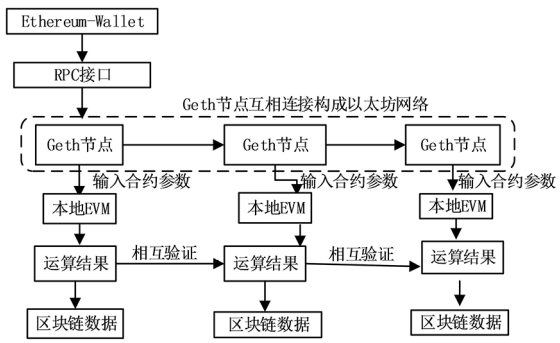

图 5 区块链智能合约执行原理

Fig.5 Execution principle of the block chain'ssmart contracts

3 基于区块链技术的数字资产确权交易模型相关算法

3.1 系统变量定义

系统中各角色、变量、算法的定义如表 1-表 3 所示。

表 1 系统角色定义

Tab.1 Role definition of the system

角色名称	缩写
密钥管理与认证中心	CA
数字资产拥有者	DO
数字内容运营商	OP
版权控制服务器	LR
数字内容服务器	DC

表 2 系统变量定义

Tab.2 Variable definition of the system

符号	含义	说明
U	用户标识	用户指数字资产拥有者
C	内容标识	第 i 个数字内容标识
EC	受保护的数字内容	
D	设备标识	设备指 OP、LR、DC、CA
γ	水印信息	

续表 2

符号	含义	说明
δ	时间戳	
P_{inf}	权限信息	
L_{inf}	许可证信息	
E_{zh}	加密内容散列值	
a_role.α_CA	系统中各角色公钥	role 为表 1 中的各角色缩写
β_role.β_CA	系统中各角色私钥	role 为表 1 中的各角色缩写
C.keyC	内容主控密钥	
C.keyE	内容加密密钥	
C.keyA	内容辅助密钥	
C.keyUK	加密内容主控密钥	

表 3　系统算法定义

Tab.3　Algorithm definition of the system

符号	含义	说明
PKS(　)	私钥签名算法	
SKS(　)	签名验证算法	
ES(　)	加密算法	
DS(　)	解密算法	

3.2　数字证书签发步骤和伪代码

在数字证书的签发流程中，用户通过模型应用端进行登录和注册，并在系统中发出申请证书的请求，数字证书认证中心向密钥管理管理中心请求加密密钥、签名密钥及签名验证算法；密钥管理中心生成加密密钥；认证中心对用户信息进行签名生成证书。

本模型中数字证书签发步骤如下：

定义 1　$U=\{u_1,u_2,\cdots,u_n\}$ 为含有 n 个数字资产拥有者的用户集合，其中 u_i 为第 i 个数字资产拥有者。

定义 2　$CA_i=\{CFV_i,CSN_i\}$ 为第 i 个证书，其中 CFV_i 为 CA_i 的证书版本号，CSN_i 为 CA_i 的证书的名称。

步骤 1　申请证书：u_i 向 CA 申请证书。

步骤 2　身份验证：CA 对 u_i 进行身份验证，若成功，则为 u_i 签发相应的数字证书 CA_i。

步骤 3　u_i 通过使用公钥 $\alpha\_u_i.\alpha\_CA$ 加密来获取私钥。

步骤 4　通过加密自己的公钥来获取私钥 $\beta\_u_i.\beta\_CA=ES(\alpha\_u_i.\alpha\_CA)$。

步骤 5　CA 对用户信息进行签名生成证书。

算法 1　数字证书签发

输入：用户集合

输出：$\beta\_u_i.\beta\_CA$

1　for each u_i in U

2　u_i 向 CA 提出申请

3　if（CA 验证 u_i=true）

4　则为用户 u_i 签发证书 CA_i，即 $U_i\rightarrow CA_i$

5　用户公开自己的公钥 $\alpha\_u_i.\alpha\_CA$，即 $U_i\rightarrow\alpha\_u_i.\alpha\_CA$

6　用加密算法 ES(　)加密用户公钥来获取私钥，即 $\beta\_u_i.\beta\_CA=ES(\alpha\_u_i.\alpha\_CA)$

7　签发数字证书

8　else

9　身份验证失败。

3.3　资产的版权注册步骤和伪代码

资产版权注册主要通过对资产添加水印和生成时间戳信息来完成。主要执行步骤如下：

步骤 1　用户下载并安装自己的数字签名证书和经过签名公钥加密的私钥。

步骤 2　用户对资产进行水印信息添加，生成 γ。

步骤 3　版权控制服务器用自己的私钥 $\beta\_LRS.\beta\_CA$ 解密得到水印信息 γ' 其中，$\gamma'=DS_{\beta\_LRS,\beta\_CA}(ES_{\alpha\_u_i,\alpha\_CA}(\gamma))$。

步骤 4　版权控制服务器向密钥管理与认证中心中申请时间戳缩略数字信息 δ。

步骤 5　密钥管理与认证中心向版权控制服务器返回时间戳缩略数字信息 δ，并保存时间戳信息 δ 到区块链的区块头中。

算法 2　生成时间戳缩略信息 δ

输入：γ

输出：δ

1　for each u_i in U

2　u_i 加密数字资产的水印信息 γ，$\gamma=ES_{\alpha\_u_i,\alpha\_CA}(\gamma)$

3　u_i 用自己的私钥进行签名，$u_i\leftarrow\beta\_LRS.\beta\_CA$

4　版权控制服务器验证签名

5 解密水印信息 γ'，$\gamma' = DS_{\beta\_LRS,\beta\_CA}(ES_{\alpha\_u_i,\alpha\_CA}(\gamma))$

6 LRS 向 CA 申请时间戳 δ

7 记录 γ 和 δ。

4 仿真分析

区块链的安全性主要考察身份验证、访问控制、加密体系和隐私、密码算法、匿名性、抗攻击能力 6 个方面。本文通过在 JAVA 环境下进行身份认证的安全性测试及密码算法性能的验证来验证模型的安全性。

4.1 实验环境

本文的实验环境为 IntelCore i5 2.53GHz，2GB 内存，实验编码实现基于 Java Security API。

4.2 实验结果

4.2.1 身份验证的安全性对比

区块链的身份验证安全性主要考察的是身份验证的方式、身份验证的场景、防止身份冒用、私钥具有完整的生命周期管理、节点的进出需要身份验证。本文所构造的模型中的区块链 A 身份验证功能全面，而 Fabric 身份验证场景单一，商业区块链 B 私钥生命周期管理不完整，具体测试结果如表 4 所示。

表 4 身份认证安全性验证

Tab.4 Security verification of identity authentication

对比项	模型中的区块链 A	Fabric	商业区块链 B
身份验证方式	密钥验证	密钥验证	密钥验证
身份验证场景	查询、转账、登录	转账	查询、转账、登录
防止身份冒用	是	是	是
私钥具有完整的生命周期管理	是，私钥有生成、分发、存储、使用以及销毁过程	是，私钥有生成、分发、存储、使用以及销毁过程	否
节点的进出需要身份验证	是	是	是

4.2.2 对比模型中不同大小数字内容的解密性能

实验环境：将数字内容大小划分为 20，40，60，80，100，120，140，160，180，200 MB，通过对比 AES 算法和 RC2 算法，进行解密性能的验证。如图 6 所示。

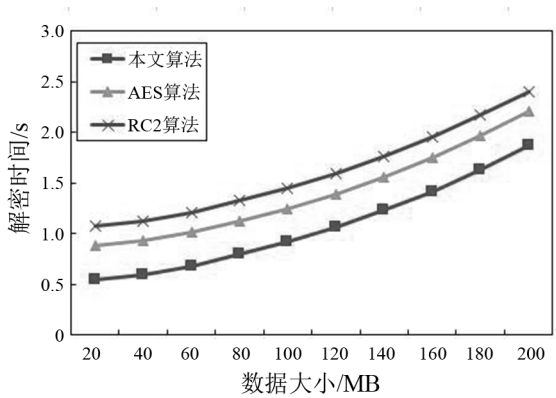

图 6 解密时间开销与内容大小的对比关系

Fig.6 Relationship between decryption time and content size

实验结果：

(1) 总体分析：随着数据内容的递增，本文算法的解密时间从 0.550 s 开始缓慢递增到 1.874 s，而 AES 算法从 0.880 s 增加到 2.204 s，RC2 算法从 1.080 s 递增到 2.404 s。

(2) 当数据量大小为 100 MB 时，本文算法的加密时间为 0.914 s，AES 算法的加密时间为 1.244，RC2 算法的加密时间为 1.444 s。当数据量增加到 120 MB 时，算法 1 的加密时间为 1.058 s，AES 算法的加密时间为 1.388 s，RC2 算法的加密时间为 1.588 s。

总之，本文所提出的算法能够非常高效的执行解密过程，而且数据量越大时，解密算法优势越明显。

5 结论

本文针对传统数字资产版权登记、签权、授权、交易等问题，研究设计了基于区块链技术的数字化资产版权确权交易模型，介绍了区块链确权

及区块链智能合约的相关理论及流程和算法。最后通过在 JAVA 环境下进行身份认证的安全性测试及密码算法性能的验证来验证模型的安全性。但系统安全性能与区块链的整体安全性仍存在较大差距。下一步将对模型中的访问控制、加密体系和隐私、匿名性、抗攻击能力进行优化验证，使模型达到更好的版权安全与交易处理能力。

参考文献：

[1] 卞鹏，金真花. 基于区块链技术的数字版权保护的创新研究[J]. 电子技术与软件工程，2018(9)：202-203.

[2] 吴健. 基于区块链技术的数字版权保护[J]. 广播电视信息，2016(7)：60-62.

[3] 程华，杨云志. 区块链发展趋势与商业银行应对策略研究[J]. 金融监管研究，2016(6)：73-91.

[4] 郑自立. 泛网时代我国数字版权保护[J]. 新闻战线，2018(4)：20-23.

[5] 牛敏. 基于区块链技术的数字版权管理模式研究[D]. 北京：北京印刷学院，2017.

[6] 董培. 区块链技术在金融业发展现状与前景展望[J]. 山西农经，2017(9)：80-82.

[7] 李良旭. 区块链技术在数字版权中的研究与应用[D]. 北京：北方工业大学，2018.

[8] 朱磊，荆磊. “互联网+”环境下数字版权保护模式[J]. 电子技术与软件工程，2017(20)：209-211.

[9] 黄俊飞，刘杰. 区块链技术研究综述[J]. 北京邮电大学学报，2018(2)：1-8.

[10] 吕坤，鲍可进. 基于区块链的数字资产交易系统设计与实现[J]. 软件导刊，2018(7)：209-213.

[11] 于韶源，杨胜春，李亚平. 基于区块链智能合约的分布式发电市场化交易机制研究[J]. 智慧电力，2018(10)：43-48.

[12] 张宁，王毅，康重庆. 能源互联网中的区块链技术：研究框架与典型应用初探[J]. 中国电机工程学报，2016(15)：4011-4023.

（特约编辑：黄家瑜）

（上接第 22 页）

[17] MOMENIFAR M R, AKHAVAN-BEHABADI M A, NASR M, et al. Effect of lubricating oil on flow boiling characteristics of R-600a/oil inside a horizontal smooth tube[J]. Applied Thermal Engineering, 2015, 91: 62-72.

[18] SCHLAGER L M, PATE M B, BERGLES A E. Performance predictions of refrigerant-oil mixtures in smooth and internally finned tubes-Part II: Design equations[J]. Ashrae Transactions, 1990, 96(1): 170-182.

[19] ECKELS S J, DOERR T M, PATE M B. In-tube heat transfer and pressure drop of R-134a and ester lubricant mixtures in a smooth tube and a micro-fin tube. Part I-Evaporation[J]. ASHRAE Transactions, 1994, 100(2): 265-282.

[20] TICHY JA, DUQUE-RIVERA J, MACKEN N A, et al. An experimental investigation of pressure drop in forced-convection condensation and evaporation of oil-refrigerant mixtures[J]. J Urology, 1986, 191: 355.

[21] ZURCHER O, THOME J R, FAVRAT D, et al. Flowboiling and pressure drop measurements for R-134a/Oil mixtures part 2: evaporation in a plain tube[J]. Hvac & R Research, 1997, 3(1): 54-64.

[22] WEI W J, DING G L, WANG K J. Measurement and correlation of two-phase frictional performance of refrigerant-oil mixtures inside small tubes[J]. Hvac & R Research, 2007, 13(2): 397-411.

[23] 胡海涛，丁国良，汪振策，等. R410A-油在 Ø7mm 水平直光管内流动沸腾阻力特性[J]. 上海交通大学学报，2007，41(3)：370-375.

（特约编辑：黄家瑜）