基于区块链的数字作品交易系统的研究

曹迪龙[1],杨文晖[2],苗 放[3]
(1.成都理工大学 信息科学与技术学院,四川 成都 610000;
2.成都理工大学,四川 成都 610000;
3.成都大学大数据研究院,四川 成都 610000)

摘 要:随着5G时代的来临,互联网应用在人类社会的方方面面已根深蒂固,而人们所拥有的数字作品也越来越多。为了解决传统的数字作品管理与交易系统存在信任依赖度高、透明度低、维护成本较高,无法完全保障数字作品的安全、无法确保著作人自身的利益等问题,通过对比特币电子现金系统的特点以及区块链技术的发展进行研究与总结,提出了一种利用区块链技术的去中心化、共识机制和链式存储等特点的方法,同时使用基于深度学习的自动定价模型,设计出一种基于区块链的数字作品自动定价与交易系统。实验结果证明,通过该系统能够在保护数字作品安全的同时,解决恶意交易、损害著作人利益等问题;可以实现用户之间的直接交易,保证数字作品完全由著作人自治。

关键词:区块链;交易系统;自动定价;去中心化;共识机制;链式存储
中图分类号:TP311.1 **文献标识码**:A **文章编号**:1673-629X(2021)04-0192-06
doi:10.3969/j.issn.1673-629X.2021.04.033

Research on Digital Works Transaction System Based on Block Chain

CAO Di-long[1],YANG Wen-hui[2],MIAO Fang[3]
(1.School of Information Science and Technology,Chengdu University of Technology,Chengdu 610000,China;
2.Chengdu University of Technology,Chengdu 610000,China;
3.Chengdu University Big Data Research Institute,Chengdu 610000,China)

Abstract:With the advent of 5G era,Internet application has been deeply rooted in all aspects of human society,and people have more and more digital works. In order to solve the problems of traditional digital works management and trading system,such as high trust dependence,low transparency,high maintenance cost,unable to fully guarantee the safety of digital works,unable to ensure the interests of the author,through the research and summary of the characteristics of bitcoin e-cash system and the development of blockchain technology,we propose a method that utilizes the characteristics of blockchain technology,such as decentralization,consensus mechanism and chain storage and design an automatic pricing and trading system for digital works based on blockchain using the automatic pricing model based on deep learning. The experiment shows that this system can not only protect the security of digital works,but also solve the problems of malicious transaction and damage to the interests of the author. It can realize the direct transaction between users and ensure the autonomy of digital works.

Key words:blockchain;transaction system;automatic pricing;decentralization;consensus mechanism;chain storage

0 引 言

传统著作者维护作品版权一般是通过实体凭证,或第三方机构认证,如通过出版社出版实体作品等。资产的流通也普遍依赖于实体书籍的售卖,这不仅导致著作者本人不能全部得到其作品所获取的所有利益,同时也面临着盗版、侵权等一系列问题。5G时代的来临,使得互联网越来越多地应用于日常生活,加之互联网技术的快速发展,资产数字化也在不断增速。理论上一切可标准化数字化的实体作品都会逐步成为数字资产,常见的数字资产包括数字积分、虚拟货币、电子优惠券、虚拟游戏道具等[1]。作品数字化实现了著作者本人与其数字作品之间形成直接联系,避免了像出版社这样的第三方代理机构对作品进行管理、出版和售卖等操作的现象。但同时也加大了著作者本人

收稿日期:2020-06-05 **修回日期**:2020-10-09
基金项目:国家重点研发计划(2016YFB0800600)
作者简介:曹迪龙(1995-),男,硕士研究生,研究方向为大数据基础研究、数据安全;杨文晖,副教授,研究方向为大数据基础研究、数据安全、虚拟现实;苗 放,博士,教授,研究方向为大数据管理、数据安全、计算机技术与应用。

对其作品权属认定的难度,由于网络开放程度大,且没有统一的数字作品存储地,这使得数字作品存在被篡改的风险,直接导致数字资产的流失。

根据统计数据显示,2019 年全国著作权登记总量达4 186 549件,同比增长 21.09%。作品登记总量达2 701 564件,同比增长 14.86%。其中科技文化领域内容被侵权最严重,每两位作者里就会有一位被侵权。从作者层面看,2019 年被侵权的作者占全体作者的23%,从内容层面上看,平均每篇内容的被侵权量为3.64 次。由此可见,数字作品权属的保护仍面临着不小的困难,如何保障著作者本人的权益成为当前网络环境中作品数字化所面临的难题。

2008 年中本聪首次发表论文《比特币:一种点对点电子现金系统》[2],并且于 2009 年发布首个比特币区块链系统。区块链技术具有去中心化、可追踪可溯源,以及分布式架构等特点,形成一种没有中心机构,多方协作且无需信任的分布式系统。由于各方互不信任,且维护同一账本,极大地降低了出现错误记录的风险。

基于区块链的数字作品自动定价和交易系统,允许任何有资格的个人或机构在系统中发布和管理数字作品。该系统采用区块链的一致性机制、分布式分类账和链式数据块存储技术,具有以下优点:①交易双方无需信任即可实现数字作品的安全交易;②系统自动制定数字作品价格,避免出现恶意交易虚拟货币,或恶意提高作品价格的现象;③利用链接存证,减小了区块链的存储压力;④实时同步分布式分类账,实现实时对账和交易结算;⑤交易数据具有安全、不可篡改的特点,且能够追踪溯源,避免了出现交易抵赖的现象。

1　区块链自动定价与交易系统相关技术

1.1　区块链技术

从本质上讲,区块链是一个共享数据库,其中存储的数据或信息具有“不可伪造”、“全程跟踪”、“可追溯”、“公开透明”和“集体维护”的特点[3]。由于区块链具有这些特点,它奠定了坚实的“信任”基础,创造了可靠的“合作”机制,使得其在金融等领域中有着广阔的应用场景。区块链技术是近年来出现的一种新技术,由去中心化和非对称数据加密、时间戳、分布式计算、共识算法等经典计算机技术组成[4-6]。区块链将加密技术与分布式消息传输协议相结合,将对账过程简化为共享的分布式总账形式,通过分散式协作队总账进行维护不仅提高了数据处理效率,还完成了信息的共享,同时确保了数据的安全,避免数据被篡改。区块链技术与传统技术相比,在持续性、兼容性、共享信息和互联性等方面具有显著优势[7]。

区块链基础架构模型如图 1 所示。

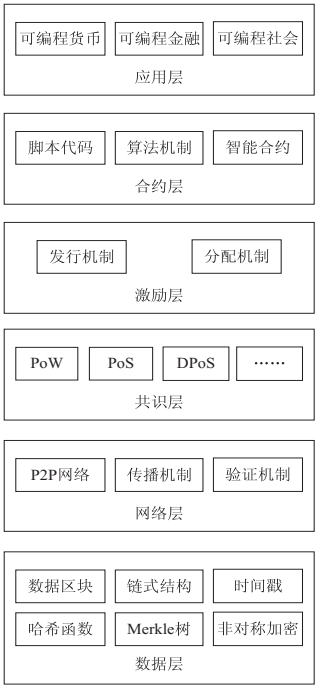

图 1　区块链基础架构模型

区块链有三种类型,即公有区块链、联合(行业)区块链以及私有区块链,其主要特点如下:

公有区块链(public block chains):世界上所有的个人和团体都可以进行交易,交易可以得到有效的确认,并且所有人都可以参与到共识过程中来。

联合(行业)区块链(consortium block chains):预先选择一些节点作为记账人,节点选择权是由某一个群体内部决定,这些节点的具有决定区块生成的权利,其他节点可以参与到交易过程,但不过问记账过程。

私有区块链(private block chains):仅仅利用区块链的总记账技术进行记账,可以是某个团体或是某个人,独享该区块链的写入权限。

1.2　共识机制

共识机制是通过特殊的节点投票,在很短的时间内完成对事务的验证和确认,是使区块链成为一种自信任体制的核心前提。区块链的自信任主要体现在不需要存在一个可信的中心化机构,用户在区块链中不需要信任交易的对方,只需要信任软件系统在区块链协议下实现交易即可。

现今区块链中的共识机制主要分为四类:工作量证明机制(proof of work,PoW),主要应用于比特币网络,但由于 PoW 在比特币网络中的应用已经吸引了全球计算机大部分的算力,同时基于 PoW 的挖矿行为还造成了大量资源的浪费,达成共识所需要的周期也较长,因此该机制并不适用于其他应用场景。权益证明机制(proof of stake,PoS),与 PoW 的区别在于不需要证明人执行一定的计算工作,只要求证明人提供一定

数量加密货币的所有权即可。但本质上与 PoW 一样，需要网络中的节点进行挖矿运算。股份授权证明机制（delegated proof of stake，DPOS），是一种新的保障网络安全的共识机制，类似于董事会投票，通过全体节点选出具有代表资格的一定数量的节点进行确认区块、维持系统有序运行。同时全体节点也具有罢免代表的权利，从而实现实时民主。DPOS 可以大大缩小参与验证和记账节点的数量，从而达到秒级的共识验证。Pool 验证池是在传统分布式一致性技术的基础上建立的，辅以数据验证机制，是当前区块链广泛使用的一种共识机制。但其也存在一些不足，该共识机制实现的分布式程度不如 PoW 机制等[8]。

1.3 分布式账本

分布式账本是基于计算能力和密码学的突破，并结合一些新的有趣算法的发现和使用，所形成的一种由大型网络中的全部参与者共享、复制和同步的数据库。该分布具有唯一性：不通过某个中心机构与各节点通信完成记录，而是有各个节点独立地构造和保持。网络中的每个用户处理同一个事务，得出各自结论，然后对结论进行投票，采用少数服从多数的方式，得到最终结论，一旦达成共识，分布式账本就会更新，所以节点都会保留自己的账本副本。

分布式账本技术颠覆传统的账本模式。第一，分布式账本是基于分布式共识算法建立的，其记录的非简单的一串数字，而是数据流；第二，记账方法属于第三方记账；第三，共享记账，所有节点在同一账本上共享及共同管理账目信息；第四，它是一种不仅可以记录资金流，同时也可以记录信息流的全信息账本。

1.4 基于深度学习的自动定价模型

深度学习算法通过对海量数据进行分割，提取出大量的隐性元素，并根据多维标签对数据进行分类，得到具有参考意义的摘要信息。根据深度学习算法可以设计一种针对数字作品的自动定价模型。模型架构如图 2 所示。

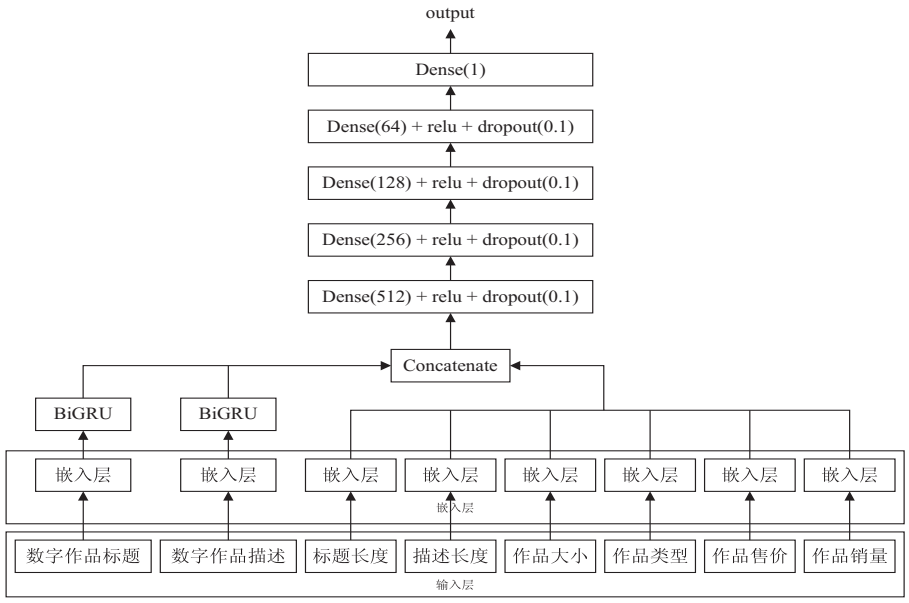

图 2 自动定价模型架构

把数字作品的相关特征输入模型的输入层，然后对不同类型的数据进行处理和嵌入。具体方法是先将数字作品标题和数字作品描述这种非结构化数据进行预处理，即分词操作，获得每个单词的索引，然后将每个词的索引转换为嵌入层中相应的词向量。对于标题长度和描述长度等这种结构化数据则转化为相应的数值，在嵌入层中转化为对应的嵌入向量[9]。

通过双向门控循环单元[10]（bi-directional gated recurrent unit，BiGRU）对得到的数字作品标题和数字作品描述的词向量序列中的文本语义进行建模，再结合其他输入数据的词嵌入进行拼接得到完整的矩阵[11]，最后使用深度人工神经网络进行特征的提取和组合[12-14]。

1.5 链式存证

区块链作为一种去中心化数据库，其数据是存储在每一个区块中，虽然区块链的账本在每个节点中都留有副本，但是区块链上的存储空间仍旧是极其宝贵和有限的。存储较大内容的数据会占用区块链的存储空间。因此对于数字作品这类可能占用空间较大的数据，采用链接存证的方式将其存储在区块链上。

链接存证是将数字作品的内容的哈希值和数字作品的 URL 地址一同进行保存上链[15]。数字作品内容的哈希值通常称为“数字指纹”，因为哈希值的长度是有限的，无论内容多大，其哈希值长度是不会改变的，因此存储这样一个哈希值对区块链来讲毫无压力。虽然数字指纹可以验证数字作品是否被篡改，但无法查

看到其原文是什么,因此将数字作品的 URL 地址与数字指纹一同上链,这样既能减小区块链的存储压力,验证数字作品真实性,同时也能够得到原文。

2　区块链数字作品自动定价与交易系统设计

区块链数字作品自动定价与交易系统主要实现个人发行、管理以及交易流通数字作品的功能。根据与数字作品的关联程度,系统业务可以分为两类:

(1)核心业务:数字作品的登记、存储、交易等业务。

(2)非核心业务:系统使用者的注册、浏览、管理等业务。

2.1　系统整体架构

该系统分为客户端和区块链节点服务器两部分。客户端主要完成非核心业务,以及递交核心业务到区块链节点服务器处理。区块链节点服务器主要完成核心业务,即执行交易过程,将交易结果打包成块,通过共识机制以后写入区块链分类账。用户注册系统时,会随机分配到一台区块链节点服务器成为该服务器中的一个节点,随着用户的增多,可以组成一个分布式的区块链节点网络。系统整体架构如图 3 所示。

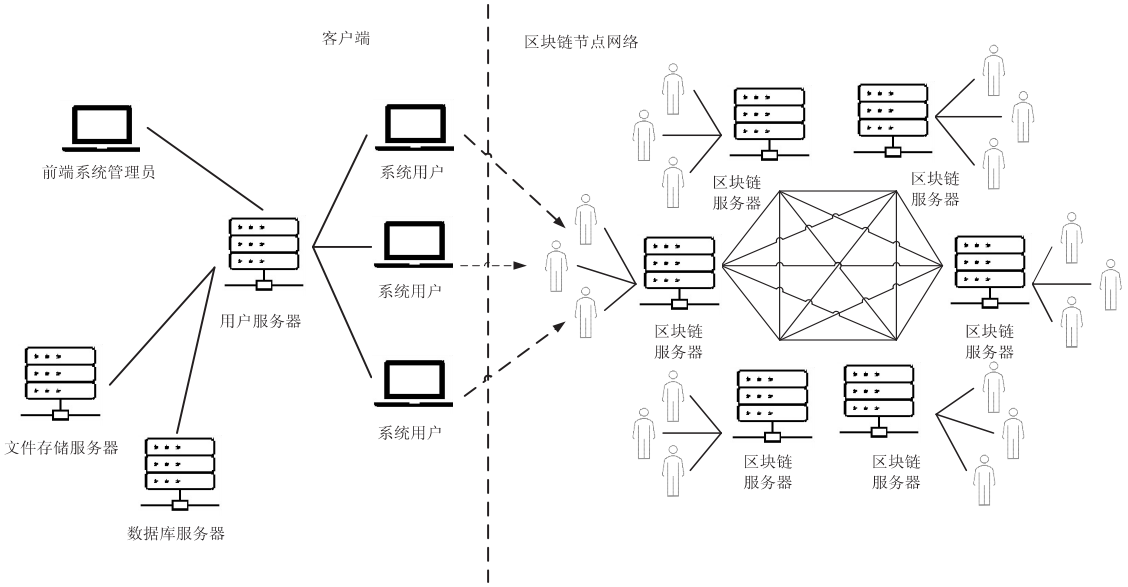

图 3　系统整体架构

与传统的集中式管理系统相比,该系统在客户端采用传统架构,而区块链服务器节点网络采用分布式架构,因此具有如下优势:

(1)节点网络采用去中心化架构,实现每个用户对其所有的数字作品进行自主管理,用户之间直接交易,无需第三方信任机构。

(2)利用 PoS 共识机制,在一定程度上减少了数字运算带来的消耗,不需要消耗大量能源挖矿,性能也得到了相应的提升,缩短了达成共识的时间,且与 PoW 有相同的容错性,更加环保。

(3)区块链节点网络执行核心业务,广播整个网络交易信息,并进行一致确认,以确保交易数据的有效性和透明度。

(4)非核心业务采用传统中心化架构,与核心业务分开管理,互不影响。

2.2　系统逻辑层次设计

系统的逻辑层可分为应用层、服务层和区块链层。应用层主要负责系统用户注册/登录、数字作品注册和交易操作。服务层连接应用层和区块链层,提供一些用户服务功能和接口等。区块链层主要包括区块链服务器、共识机制、网络通信模块等。三层结构组成一种自下而上的以区块链为核心的逻辑层次,系统整体逻辑层次如图 4 所示。

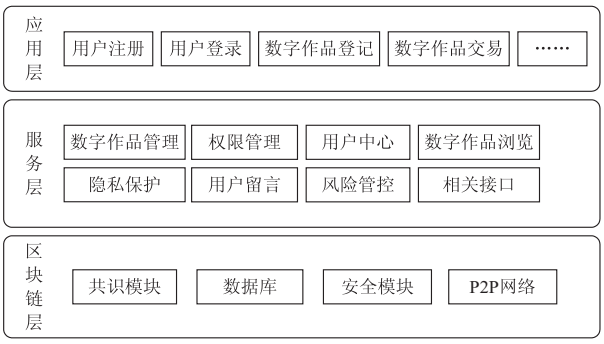

图 4　系统整体逻辑层次

3　区块链数字作品自动定价与交易系统实现

3.1　系统业务逻辑

该系统中的非核心业务与一般中心化管理系统相

类似,即用户注册登录等信息保存数据库中,调用接口执行相应命令。核心业务主要有两部分,一是数字作品的登记上链,用户将数字作品在客户端上传存储到区块链节点区块中,这时区块链系统会接收消息并广播全网,达成共识后,记录该数字作品到账本中;二是数字作品的交易流程,用户在客户端提交交易申请,区块链系统接收到申请后会执行交易流程,并广播全网达成共识,记录交易信息到账本中,返回交易结果给客户端。客户端处理非核心业务,并获取交易结果,将最终的交易信息返回给用户。具体业务逻辑如图 5 所示。

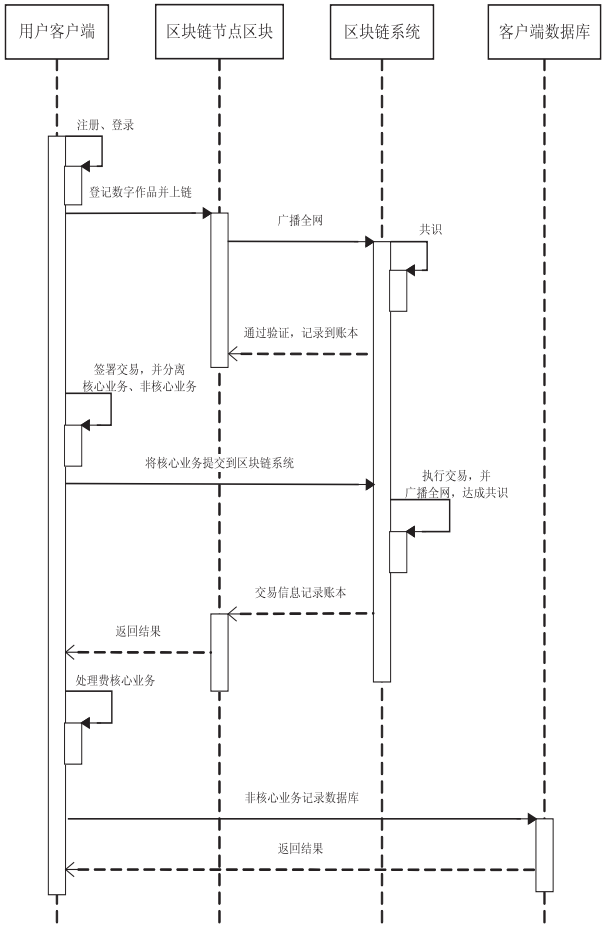

图 5 系统业务逻辑

3.2 系统实现

3.2.1 用户注册

当用户在客户端注册时,将生成一对公钥和私钥,私钥用户自己留存,公钥由系统直接编码形成用户 ID,记录在客户端数据库中,同时将公钥发送给某个区块链服务器。区块链服务器对用户的注册信息进行验证,验证通过以后,签名并存储用户信息到区块链中,成为链上的一个节点块,区块链系统广播整个网络,达成共识并记录到账本中,完成用户注册。

3.2.2 数字作品登记

用户需要在客户端对数字作品进行登记,登记信息包括:数字作品标题、数字作品描述(简介)、作品类型和大小。系统会根据用户输入的数据使用自动定价模型,得到数字作品的价格,该价格不可更改。同时,还需要用户上传数字作品,客户端会将数字作品进行哈希加密(SHA256),并上传至文件存储服务器,返回文件 URL 地址。然后客户端会将数字作品的哈希值和 URL 地址,即数字作品的链式存证,提交给区块链系统。区块链系统收到数据后进行全网广播、共识,并记录到账本中,完成数字作品登记。

3.2.3 数字作品交易

用户提交交易申请到区块链系统,系统会首先验证交易发起者的身份,然后查询其账户余额是否充足,如果余额不足则交易失败;如果余额充足则返回交易结果。交易流程如图 6 所示。

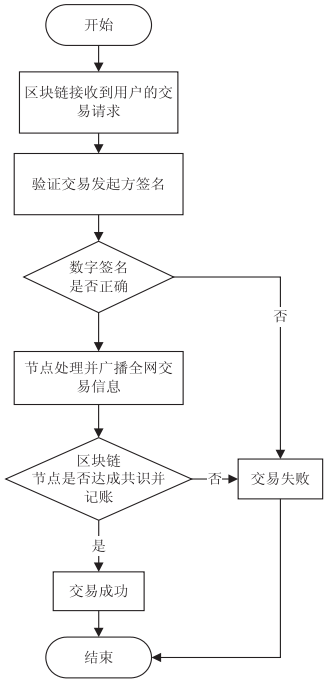

图 6 系统交易流程

4 系统测试与分析

系统测试主要是对系统性能和业务流程进行测试。采用黑盒测试技术对系统业务流程进行测试,模拟从用户注册到交易完成一系列操作,以检验系统业务流程是否完整。系统性能测试则采用实验的方式,得到从并发交易开始到完成交易时,系统的交易处理率和交易平均延时。

利用三台虚拟机搭建分布式测试环境,每台虚拟机采用相同操作系统和系统设置。在局域网中测试了系统的性能,并采用了相同的算法机制,以减少网络环境和算法对实验结果的影响。

系统在一定时间内成功完成和提交的事务数与事务总数的比值即为事务处理率。系统完成一个事务所

花费的平均时间就是该事务的平均延迟。计算公式如下:

事务平均延时=事务总延时/事务笔数

事务处理率=正常通过事务数/总事务数

根据测试得到的数据结果可知,在具有三个节点的分布式区块链网络中,当使用 PoS 共识机制时,平均事务延迟随着并发事务数量的增加而增加,同时交易处理率随之下降。当并发交易数在 350 笔时,交易处理率开始下降,交易平均延时开始增加。综上所述,该系统在接收并发交易数据小于 350 笔时,系统性能达到最好的效果,此时系统的单笔交易延时为 5 s ~ 10 s。

5　结束语

针对传统的中心化系统存在的信任依赖度高、透明度低、维护成本较高等缺点,设计了一种基于区块链的数字作品自动定价与交易系统,在保障数字作品著作人权益的同时,能够实现用户之间直接交易。对系统所使用的技术及其设计框架和业务流程进行了介绍,该系统具有无需第三方信任机构、自动制定数字作品价格、使用链接存证等特点。最后对系统性能进行了测试和分析,由测试结果可知虽然系统可以达到预期的效果,但距离实际应用的要求仍然有着不小的距离。因此,下一步将在充分发展系统优势的同时,解决系统所存在的问题,实现更加理想的交易处理能力。

参考文献:

[1] 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,2018,17(7):209-213.

[2] NAKAMOTO S. Bitcoin:a peer-to-peer electronic cash system[J]. Consulted,2008(1):2645-2652.

[3] 孙善勇,张玉清. 区块链技术[J]. 首都师范大学学报:自然科学版,2020,41(2):81-84.

[4] 袁　勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报,2016,42(4):481-494.

[5] 周国良. 基于区块链的二手房交易系统的设计[J]. 信息与电脑:理论版,2020,32(1):79-82.

[6] 邵晓蓓. 区块链数据交易系统的设计与实现[D]. 济南:山东大学,2019.

[7] NIZAMUDDIN N,HASAN H,SALAH K,et al. Blockchain-based framework for protecting author royalty of digital assets[J]. Arabian Journal for Science and Engineering,2019,44(4):3849-3866.

[8] 区块链共识机制的规则特点:共享、共识与共赢的制度基础[J]. 软件,2018,39(6):228-230.

[9] 黄　贺. 基于深度学习的商品自动定价模型研究[J]. 现代商贸工业,2019(9):188-190.

[10] 郑　诚,薛满意,洪彤彤,等. 用于短文本分类的 DC-BiGRU_CNN 模型[J]. 计算机科学,2019,46(11):186-192.

[11] GAO Huang,ZHUANG Liu,VAN DER MAATEN L,et al. Densely connected convolutional networks[EB/OL]. (2018-01-28)[2020-03-22]. https://arxiv.org/abs/1608.06993.

[12] 曹鲁慧,邓玉香,陈　通,等. 一种基于深度学习的中文文本特征提取与分类方法[J]. 山东科学,2019,32(6):106-111.

[13] 黄立威,江碧涛,吕守业,等. 基于深度学习的推荐系统研究综述[J]. 计算机学报,2018,41(7):1619-1647.

[14] 黄　晋,蔡　钰,赵曦滨,等. 一种基于深度学习的混合区块链模型构建方法:2018115628859[P]. 2019-05-03.

[15] 刘格昌,李　强. 基于可搜索加密的区块链数据隐私保护机制[J]. 计算机应用,2019,39(S2):140-146.