

丁勇<sup>1</sup> 相恒奎<sup>1</sup> 袁方<sup>2</sup> 罗得寸<sup>1</sup> 刘林刚<sup>1</sup> 邹秀清<sup>1</sup> 唐晨钧<sup>1</sup>

## 基于区块链的论文评审及追溯系统

### 摘要

移动互联网时代,人们在学习专业知识信息的方式越来越便捷的同时,学术论文抄袭、造假等问题也日益受到关注.而随着以比特币为主要代表的数字货币的出现,其底层用到的区块链技术也快速地进入人们的视线.本文根据区块链技术的去中心化、去信任、可追溯等特性,提出了一种基于区块链的论文评审及追溯系统.本系统在解决中心化的系统带来的高成本、安全性等问题的同时,对论文以及论文发布审核的过程进行检索、记录、存储,使得论文的发布检索审核等过程变得安全、可以追溯.

### 关键词

区块链;去中心化;论文评审;追溯

中图分类号 TP13

文献标志码 A

收稿日期 2019-06-30

资助项目 国家自然科学基金(61772150,61862012);广西重点研发计划(AB17195025);广西自然科学基金(2018GXNSFDA281054,2018GXNSFAA281232);国家密码发展基金(MMJJ20170217)

### 作者简介

丁勇,男,博士,教授,主要研究方向为信息安全、大数据、物联网等. stone\_dingy@126.com

### 0 引言

随着比特币<sup>[1]</sup>等加密数字货币的兴起,其底层用到的区块链技术也越来越受到重视.区块链作为比特币的技术支撑,具有去中心化、可靠性高、匿名、可追溯、安全可信等特性<sup>[2]</sup>.自2008年,由中本聪发表的《比特币:一种点对点式的电子现金系统》<sup>[3]</sup>,阐述了基于P2P网络技术、加密技术、时间戳技术、区块链技术等电子现金系统的架构理念,其去中心不需要信任的点到点的交易体系方法即比特币,已经稳定运行了10年之久.而随着区块链技术的不断成熟,各国政府也注意到了区块链技术的发展潜力.对区块链技术的发展前景寄予厚望<sup>[4]</sup>.目前对于区块链,许多国家都颁布了扶持政策,大力支持区块链技术在各个行业领域落地应用.

目前,区块链的落地应用已经有很多的尝试以及案例.李博等<sup>[6]</sup>通过分析区块链的核心要素,对法定货币、跨境支付、数字票据、供应链金融、证券交易等金融方面与区块链的结合进行了详细的分析.孙韵秋等<sup>[7]</sup>将高校的成绩数据管理与区块链结合,为高校数据的安全性等问题提出了新的解决思路.刘家稷等<sup>[8]</sup>将区块链应用到溯源问题提出了双链系统,在解决产品标签复制、滥发以及产品质量问题责任溯源的同时,使系统高效运行.巫岱玥等<sup>[9]</sup>将多链结构用于具有分层权限的信息系统上,通过数据保护使得信息系统的具有更高的安全性.田秀霞等<sup>[10]</sup>将区块链与电能交易相结合,提出了一种解决电能交易中存在的隐私泄露、交易安全性等问题的解决方案.

利用区块链解决系统中数据的安全性问题,也是区块链重要的应用点.祝烈煌等<sup>[11]</sup>在分析了区块链的交易数据被攻击者挖掘利用,会面临隐私泄露的风险,提出了以混币机制来保护数据隐私.王继业等<sup>[12]</sup>将数据安全共享与区块链结合,提出了一种解决企业内部和企业之间的数据安全共享的可信网络构建方案.闫树等<sup>[13]</sup>将区块链的特性与数据流通结合,为存证环节、数据的溯源以及如何实现智能合约提供了思路.

此外,将区块链应用于溯源领域,也是目前区块链技术落地的研究热点.王玉娟等<sup>[14]</sup>通过分析当前的食品安全环境问题,使用商品条码将商品的追溯数据信息存入区块链中,利用区块链技术使得存入的数据不可篡改,提高了供应链的信息透明度.郭珊珊<sup>[15]</sup>在分析现有的供应链溯源方式不足之处的基础上提出了新的解决方案,将链上

1 桂林电子科技大学 计算机与信息安全学院,桂林,541004

2 外交部通信总台,北京,100016

的交易角色作为节点共同维护整个网络,避免了数据的篡改,使得溯源信息的查询结果变得更加可信。

杨云勇等<sup>[16]</sup>提出的数据溯源方案将区块链与其他安全技术结合,安全 RFID 产品防复制等特点与区块链的数据防篡改、分布式存储以及点对点传输的特点提高了溯源链的安全性、可靠性以及信息的可信性。此外,刘晓云等<sup>[17]</sup>将物联网技术与区块链技术进行了结合并应用到了农产品溯源问题上,解决了物联网技术无法解决的数据的信任问题,使得信息更加安全可靠。

信息化的高速发展也在刺激着数据库软件市场规模快速增长。尽管传统数据库具有查询迅速、数据结构化、数据冗余度小和共享性好等优势,但其本身的架构、认证与控制方式依然存在诸多风险和隐患。传统数据库使用客户端-服务器端架构,数据存储为中心化的服务器上,一旦服务器机房遇到断电、硬件设备故障,就会出现数据库无法访问的问题。分布式数据库技术<sup>[5]</sup>,能一定程度上规避上述问题,但其抗风险能力仍不及区块链方式存储。而且,在传统的数据库中普通用户难以确保从数据库中获取的数据没有被损坏或者篡改,也很难得知数据被修改的历史记录。目前大多数的学术论文数据库都是中心化的,因此,如何维护学术论文数据库,使得存放在学术论文数据库内的数据更加安全可靠,对促进学术建设具有重要的意义。针对上述问题,本文提出了使用区块链技术作为系统底层的方案,利用区块链的特性,为解决学术论文在评审以及发表过程中的信任问题以及学术造假的责任追溯问题提供技术支持,使得学术论文的评审及发表等过程更加透明化。

本文针对传统的中心化的系统在论文发表过程中存在的安全性、信任以及责任追溯等问题,提出了一种基于区块链的论文评审及追溯系统,在解决中心化系统高成本、安全性差等问题的同时,使得论文发布审核等过程变得透明、安全、可追溯。

## 1 区块链的概念和关键技术

### 1.1 区块链的概念

区块链是在去中心化系统中各个节点共享的数据账本,每个分布式节点都可以通过特定的哈希算法和 Merkle 树,将收到的数据封装到一个带有时间戳的区块中,并根据上链的原则链接到当前最长的主链上。每个区块一般包含区块头、区块体两部分。区块头里存放了当前的版本号、前一个区块的地址、当

前区块的目标哈希值、当前区块共识过程的随机数、Merkle 根等信息<sup>[18]</sup>(图 1)。

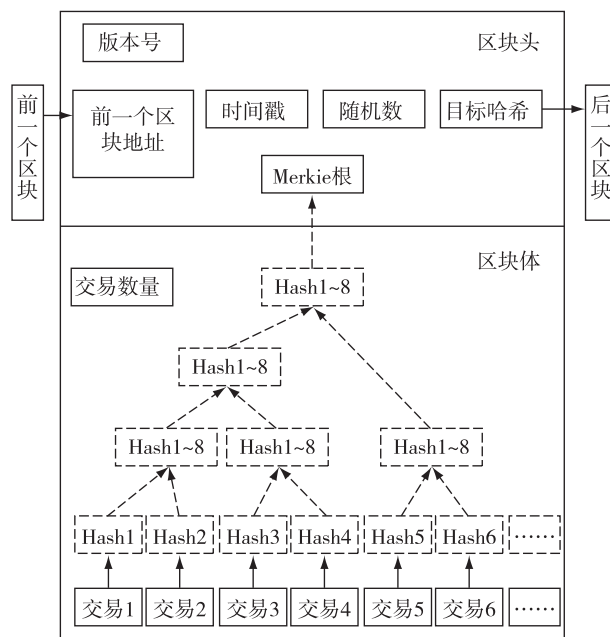


图 1 区块链结构示意图

Fig. 1 Blockchain structure

### 1.2 底层数据

在区块链系统中,底层的原始数据并不是直接写入而是需要被进一步处理才能写入区块内的。时间戳则是用来确定区块的写入时间,可以作为区块数据的存在性证明,形成不可篡改不可伪造的分布式账本。将时间戳加入区块链更为重要的意义在于为基于区块链技术的互联网和大数据增加了一个时间维度,使得通过时间戳来追溯重现历史成为可能。

Merkle 树是区块链技术的重要组成部分,它将交易信息运算后的散列值按照二叉树形式结构组织起来保存在区块中。它会将区块链数据分组进行散列函数运算,然后将新的散列值放回,再重新取两个数据进行运算,直到剩下唯一的 Merkle 根。Merkle 树有着良好的扩展性,不管交易数据如何都可以生成 Merkle 树,它的查找算法时间复杂度很低,可以极大地降低运行时的资源占用,使得轻节点称为可能,不用保存全部的区块链数据就可以验证交易的合法性。

### 1.3 分布式账本

分布式账本是一种在网络成员之间共享、复制和同步的数据库,它记录网络参与者之间的交易,比如资产或数据的交换。网络中的参与者根据共识原则来制约和协商对账本中的记录的更新,没有第三

方的仲裁机构.在分布式账本中的每条记录都有一个时间戳和唯一的密码签名,使得账本成为网络中所有交易的可审计历史记录.

#### 1.4 P2P 网络

对等网络,又称点对点技术.它没有中心服务器,而是依靠用户群交换信息的互联网体系.对等网络中,每个用户端既是节点又有服务器的功能,任何一个节点无法直接找到其他节点,必须依靠其用户群进行信息交流.对等网络的一个主要优势就是让网络中的客户端也能提供资源.对等网络的分布特性会通过多节点上复制数据,增加系统的健壮性.在一般型的对等网络中,节点不需要依靠一个中心索引服务器来发现数据,系统也不会出现单点崩溃<sup>[19]</sup>.

区块链的网络也采用 P2P 组网方式来达到去中心化的目的,网络中的节点之间以扁平式拓扑结构相互连通和交互,节点间的地位均对等,不存在任何中心化的特殊节点.

#### 1.5 共识机制

区块链中的共识机制是一套制度,用来维护系统的运作顺序与公平性,统一区块链的版本,并奖励提供资源维护区块链的使用者以及惩罚恶意的危害者.区块链上交易的记录权与奖励的发放权需要全网节点共同参与投票,只有得到了全网大多数节点的同意,才能最终确定,通过这样的规则保证整个网络的安全性、交易的有效性,使得整个网络在这套规则的框架内正常地运行下去.

在区块链的整个系统框架中,信任是网络运行的基础,而共识机制是维护信任的机制.共识机制最大的用处在于用全网节点共同监督、记录交易的方式来解决不信任的问题.区块链的共识机制分为以下几种:PoW(工作量证明)、PoS(权益证明)、DPoS(股份授权证明)、PBFT(实用拜占庭容错).其中 PoW 是指付出的工作量越大,则能获得记账奖励的概率就越大.PoS 则是持有的币越多,当前挖矿难度越低,获得奖励的概率就会越大.DPoS 是以太坊中,节点通过投票选出节点来运营网络.PBFT 则利用拜占庭容错机制,是联盟链和私有链中较为常用的高效的共识机制<sup>[20]</sup>.

#### 1.6 智能合约

智能合约是部署在区块链上的去中心化、可信息共享的程序代码,是一种旨在以信息化方式传播、

验证或执行合同的计算机协议<sup>[21]</sup>.签署合约的参与方就合约的内容达成一致,以智能合约的形式部署在区块链上,无需第三方信任机构即可自动化地执行合约.智能合约减少了人工的参与,保证系统可以根据提前设计好的规则安全执行,降低了交易的成本.

## 2 系统模型设计

### 2.1 系统模型

本文提出一种基于区块链的论文评审及追溯系统(图2).系统主要包括用户注册模块、论文投放模块、重复检索模块、论文评审模块、信用记录模块以及论文价值判断<sup>[22]</sup>模块.用户通过论文投放模块将需要发表的论文投放到对应的论文链上,当论文通过评审模块后会产生关联于该论文的信息链,存放论文的信息.论文评审模块根据共识机制原理对论文进行评审决议是否可以发布.此外论文的评审模块根据一定的激励抢答机制,向具有相关领域的有评审资格的用户推送评审,参与评审的用户则可以获得一定的信用积分作为回报.

进行评审前,论文先进入重复检测模块,该模块会先检测论文作者的信用记录模块是否最近有过不良记录的标记,如果存在不良记录则会在一段时间内限制用户发表论文,限制期限过后才允许该用户再次发表论文,且不良记录的标记不会被取消.

当用户在成功发表论文后,会对用户以及参与评审的用户奖励一定的信用积分作为回报,同时在其他用户阅读该用户的论文时,也会支付作者一定的信用积分.系统将根据参与评审的评审人信用等级、用户自身的信用等级以及用户对该论文的满意度作为论文价值判断机制的重要因素,且信用积分只能通过发表论文以及参与评审获得.

### 2.2 设计原则

本文所提出的一种基于区块链的论文评审及追溯系统,其设计遵循如下规则:

1)奖励用户发表论文以及专家参与评审的行为.对于用户发表论文的行为进行一定的信用积分奖励,这里的信用积分是一种虚拟数字代币,且只在本系统内部可以使用.用户在参阅别人发表的文章后,可以给予论文发表者一定的信用积分作为回报,本系统的发表论文以及参与论文评审可以看作是一种“挖矿”行为,这种方式让用户以及论文评审者都可以用自己的知识获得一定的收益,并用这些收益

学习更多本系统内的学术文章。

2) 信用积分根据共识机制中定义的规则产生. 为了尽可能地降低人为因素对系统的干扰, 通过分析当前发表论文的数量, 使用智能合约根据经济规则管理当前系统内存在的信用积分数量以保障系统内部可以稳定地运作, 避免恶意交易炒作信用积分等行为, 让系统的参与者更加注重学术交流而不是利益。

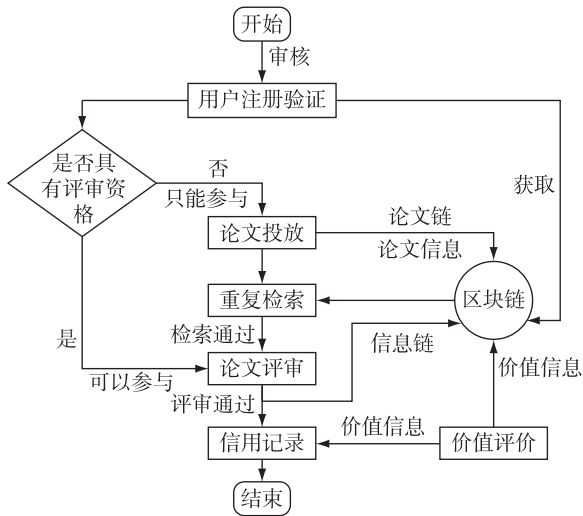


图2 系统模型设计  
Fig. 2 System model design

### 2.3 系统的总体架构设计

基于区块链的论文评审及追溯系统主要利用区块链去中心化、去信任的特点, 通过数据加密算法、分布式的共识机制以及点对点的对等网络传输协议等手段, 在分布式系统中实现基于去中心化的点对点交易. 本系统底层采用公有链的方式搭建, 在此基础上架设论文评审及追溯系统, 该系统包括用户注册认证模块、论文投放模块、重复检索模块、论文评审模块、论文价值判断模块以及信用记录模块. 系统运行流程如下: 用户通过用户注册模块进行注册以及选择是否具有评审资格, 当用户需要发表论文时, 会进入论文投放模块进行处理, 该模块会产生相关的论文链存放论文信息, 此后进入论文的重复检索模块检索该论文的内容是否存在抄袭等学术不端的行为. 论文通过重复检索模块后会进入论文的评审模块, 该模块在得到该领域足够数量的评审专家响应后, 对论文进行评审, 并且评审成功后会产生关联于该论文的信息链, 用户在发表论文评审通过以及专家在参与评审后将会获得系统奖励的一定数量的信用积分作为奖励, 最后通过系统的信用记录模块

记录到用户的账户中(图3)。

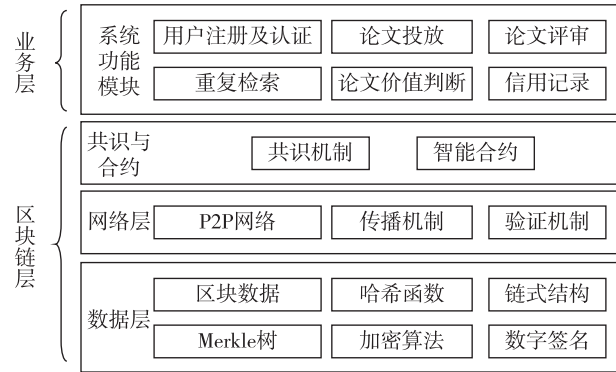


图3 系统设计框架  
Fig. 3 System design framework

## 3 系统详细设计

### 3.1 系统的功能模块设计

本系统由6个模块组成, 具体包括用户注册认证模块、论文投放模块、论文评审模块、重复检索模块、论文价值判断模块以及信用记录模块. 以下对各个模块进行详细阐述。

#### 1) 用户注册认证模块

用户注册认证模块主要功能是在用户注册时根据用户输入的实名信息进行验证, 判断用户是否具备系统的注册资格(图4). 注册时, 系统会判断该用户是否已经注册或是否是被系统标记处理掉的用户, 如果存在上述情况则不允许用户进行注册. 当用户注册完成后, 可以自己选择是否认证评审资格参与论文评审, 系统会根据用户填写的信息进行认证. 用户本身的学术地位越高, 注册后的评审人等级就越高. 用户认证评审资格通过后, 系统会根据用户所在的专业领域推送对应的需要评审的论文, 而用户对于该类推送有选择同意参与评审以及拒绝的选择权利. 当用户注册完成以及完善好用户信息后, 系统会产生与该用户绑定的信用记录模块, 用于记录用户发表论文或者参与评审所获得的信用积分, 以及标记用户是否有过学术不端等不良行为。

#### 2) 论文投放模块

用户在选择发表论文时, 会通过论文投放模块将论文投放到对应的论文链上. 当论文通过评审模块后, 系统会根据已经通过评审的论文产生关联于该论文的信息链用以存放审核通过后的论文信息, 以便系统中的其他用户进行检索和学习. 论文链以及信息链即底层采用了区块链技术将论文信息存储

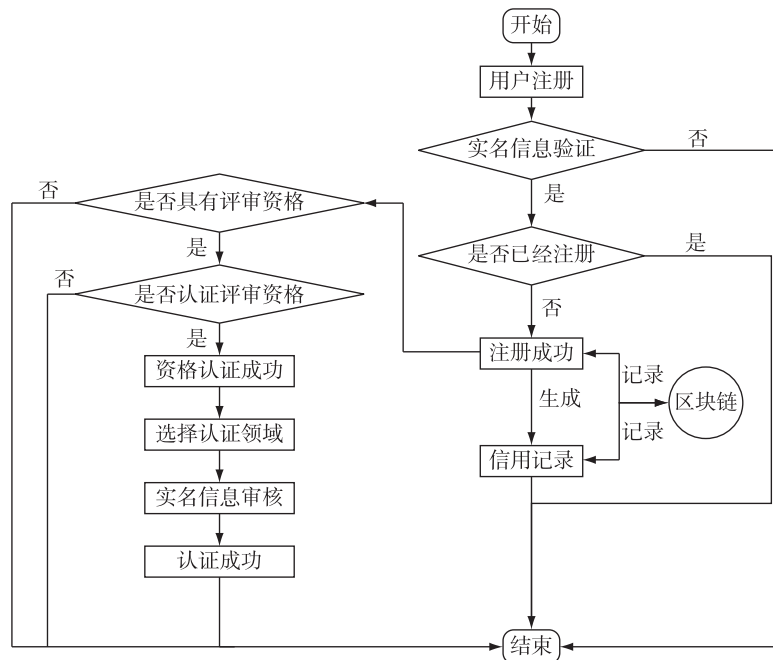


图4 用户注册过程

Fig. 4 User registration process

在其节点上组成的链,利用区块链不允许删除和修改已经存储在节点的数据的特性,保护论文的信息。

### 3) 重复检索模块

重复检索模块根据用户提交的论文进行检索,检测论文是否存在抄袭等学术不端的行为,系统会将检测结果标记并记录到该用户的信用记录模块。一旦用户存在学术不端的行为,系统将扣除用户一定数额的信用积分并禁止用户在一段时间内再次发表论文。

### 4) 论文评审模块

论文的评审方式引入区块链中共识机制<sup>[23]</sup>的原理。当具有资格的对应领域的用户选择参与评审后,该用户所在的节点先对论文链上的论文进行独立验证。每个评审人所在的节点收到评审的论文信息后,都会根据自己的判断标准对该论文进行评审并给出评审意见,然后用户会根据评审返回的结果做出回应。

当论文通过评审节点的验证后,该节点会将验证通过的论文信息放入本地的交易池,并将该论文通过验证的消息广播给其他参与评审的节点。其他的评审节点在收到论文验证通过的消息后,同样会各自做自己节点的论文评审验证,验证论文评审通过后同样也会放在自己的交易池中,并继续广播给其他节点。当该论文评审通过的消息广播到所有参

与评审的节点并被节点所保存后,所有的参与评审的节点达成了“该论文评审通过”的共识。而当评审的节点决定论文的评审不通过时,则评审结果不会放在交易池也不会广播出去。

经过一段时间后,每个节点的交易池会收到许多有效但是还未确认的评审信息,这些信息会组装成一棵 Merkle Tree。类似于比特币,信用积分的生成也是从组装进 Merkle Tree 的第一笔交易中产生。组装好 Merkle Tree 后,就会得到 Merkle Root,然后结合区块头等信息计算出区块的哈希值。当某节点计算出了符合要求的区块哈希值后,将此区块装到对应的论文的信息链上,论文发表成功(图5)。

### 5) 论文价值判断模块

系统的论文价值判断模块用于合理判断分析论文的价值,对于贡献价值较高的论文,系统会额外给用户一定的信用积分作为奖励,促进学术氛围建设。论文的价值设置由以下因素决定:参与评审的评审人信用等级、用户自身的信用等级、用户对该论文的满意度。具体如下:

a. 参与评审的评审人信用等级:用户将论文发布在初始的论文链上,进入论文评审模块并由系统推送给评审人员,由评审人员判断论文是否存在价值而决定是否评审。参与评审的人员在注册时会根据自身的学术地位被标注为不同等级的评审人,评

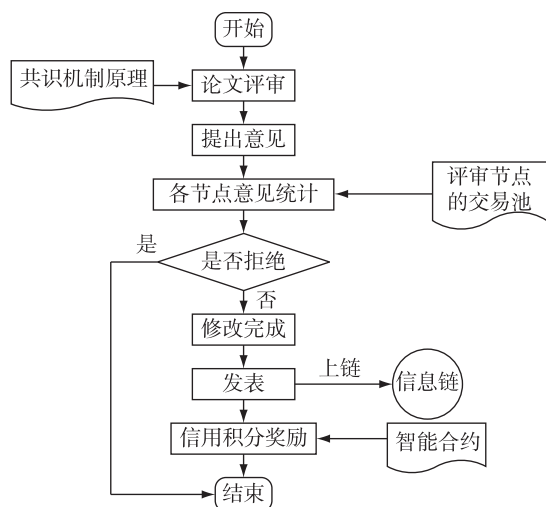


图5 评审处理流程

Fig. 5 Review process

审人的等级越高则侧面反映论文的价值越高.因此,不同等级的评审人员,对论文价值的判定占有不同的权值比重.

b.用户自身的信用等级:由于系统的信用积分只能通过发表论文、参与评审以及论文被其他用户阅读后支付获得,所以当用户自身累积的信用积分达到一定数额时,可以为用户提升信用等级.不同用户的信用等级,对论文的价值判定占有不同的权值比重.

c.用户对该论文的满意度:当论文发布后系统会奖励用户一定的信用积分,在其他用户阅读该论文时也会根据自己在阅读论文后的收获选择给论文进行满意度评价.为了尽可能地避免论文出现刷分的情况,用户在阅读完论文简介后,需要支付一定的信用积分再选择阅读全文.所以将其他用户对该论文的满意度作为参考,也可以反映出论文的价值.

论文的价值会根据以上的因素动态变化,将上述的论文价值判断因素根据分配的不同权重,求出总和即为该论文的价值.

#### 6) 信用记录模块

信用记录模块可以记录用户的信用值、信用值使用记录、用户信用等级以及是否有不良记录标记等信息,此外还会根据论文价值判断模块计算出用户发布的论文的价值,来提升用户的信用等级.

### 3.2 系统平台设计

本系统的底层通过使用区块链技术,在解决中心化的存储学术论文带来的高成本、安全性等问题的同时,将论文以及论文发布审核的过程进行检索、

记录、存储,使得论文的发布检索审核等过程变得安全且可以追溯.系统平台的核心内容如下:

#### 1) 分布式存储

用户将论文投稿后会产生相应的论文信息并将其存放到论文链上,主要存放作者投稿论文题目、作者、时间以及研究方向等信息.当论文最后通过审核发布时,则会将最终的结果放到论文的信息链上,供需要的用户查阅.此外还会将作者的信息、信用值情况等信息也存放到链上,使得用户信息、信用积分、论文的发表以及审核过程等信息变得可追溯.

#### 2) 共识机制

系统底层采用 DPoS 共识机制.它在权益证明 (PoS) 的基础上增加了“委托”,通过投票选举出代表节点来运营网络,用专业运行的网络服务器来保证区块链网络的安全和性能.通过选举,将记账权力委托给一小群超级节点,它将大幅缩小参与验证和记账节点的数量,可以达到秒级的共识验证.

#### 3) 智能合约

本文信用积分的交易将通过智能合约来完成<sup>[24]</sup>,只有用户的信用积分足够支付阅读论文时,才可以进行阅读.使用智能合约根据经济学原理控制系统的信用积分数量,增强系统的健壮性.根据论文的价值判断模块实现论文价值的动态变化,使用智能合约控制用户的信用等级.用户发表的论文一旦存在学术不端等情况被标记在信用记录模块,则会通过智能合约对该用户进行一定的信用积分处罚,并限制该用户在一段时间内进行论文投放.

## 4 系统性能分析

### 4.1 系统易用性分析

整个系统分为底层的区块链层和上层的业务层.业务层的处理流程贴合实际,与传统的中心化的系统操作并无差异.用户也主要是接触业务层的人机交互界面,根据界面的人性化提示就可以进行操作,满足系统的易用性要求.

### 4.2 系统可扩展性分析

系统的底层与业务层都是模块化的设计.当论文的评审与追溯出现新的需求时,可以根据新的需求对业务层进行扩展,然后对底层的区块链层添加相关的智能合约即可,并不会对原有的功能造成影响,具有很好的可扩展性.

### 4.3 系统健壮性分析

分布式账本本身就是在 P2P 网络内复制、同步

和共享,当其中的某个节点账本损坏时,并不能影响系统的运行,其他节点上的数据仍可以使得系统正常地运行.因此系统具有较高的容错能力和较高的健壮性.

#### 4.4 系统安全性分析

系统底层采用区块链技术,使得系统的数据存储由原来的中心化存储变成分布式存储,数据被破坏的可能性大大降低.数据经过密码学算法、时间戳等技术处理存放在链上,保证了数据不可篡改以及可追溯,相比于传统的存放方式,本系统更加安全可靠.

## 5 总结

本文提出基于区块链的论文评审及追溯系统,旨在降低传统论文存放方式的风险,提高论文评审的公开透明性以及学术不端情况出现后的追责问题,有利于促进学术风气建设,促进学术交流.随着区块链技术的快速发展,区块链技术的落地应用也从摸索阶段不断地走向成熟.未来区块链技术不断更新,更加适用于解决安全性、信任、追溯等问题后,可以更进一步优化本系统,构建良好学术风气.

## 参考文献

### References

- [ 1 ] 贾丽平.比特币的理论、实践与影响[J].国际金融研究,2013(12):14-25  
JIA Liping.Bitcoin: theory, practice and effect[J].Studies of International Finance,2013(12):14-25
- [ 2 ] 何蒲,于戈,张岩峰,等.区块链技术与应用前瞻综述[J].计算机科学,2017,44(4):1-7,15  
HE Pu, YU Ge, ZHANG Yanfeng, et al. Survey on blockchain technology and its application prospect [ J ]. Computer Science, 2017, 44(4): 1-7, 15
- [ 3 ] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL].[2019-06-29].<https://bitcoin.org/en/bitcoin-paper>
- [ 4 ] 中国区块链技术和产业发展论坛.中国区块链技术和应用发展白皮书[M].工信部,2018  
China Block chain Technology and Industry Development Forum.China blockchain technology and application development white paper[M].Ministry of Industry and Information Technology of P.R.C.,2018
- [ 5 ] 杨东,谢菲,杨晓刚,等.分布式数据库技术的研究与实现[J].电子科学技术,2015,2(1):87-94  
YANG Dong, XIE Fei, YANG Xiaogang, et al. Research and implementation of distributed database technology [ J ]. Electronic Science & Technology, 2015, 2(1): 87-94
- [ 6 ] 李博,郑博,郭子阳,等.区块链技术在金融方向应用的发展及展望[J].应用科学学报,2019,37(2):151-163  
LI Bo, ZHENG Bo, GUO Ziyang, et al. The state-of-the-art blockchain applications in finance: progress and trends [ J ]. Journal of Applied Sciences, 2019, 37(2): 151-163
- [ 7 ] 孙韵秋,王启春.基于区块链技术的高校成绩管理系统[J].密码学报,2018,5(5):568-578.  
SUN Yunqiu, WANG Qichun. University score management system based on blockchain technology [ J ]. Journal of Cryptologic Research, 2018, 5(5): 568-578
- [ 8 ] 刘家稷,杨挺,汪文勇.使用双区块链的防伪溯源系统[J].信息安全学报,2018,3(3):17-29  
LIU Jiaji, YANG Ting, WANG Wenyong. Traceability system using public and private blockchain [ J ]. Journal of Cyber Security, 2018, 3(3): 17-29
- [ 9 ] 巫岱玥,余祥,王超,等.基于区块链的信息系统数据保护技术研究[J].指挥与控制学报,2018,4(3):183-188  
WU Daiyue, YU Xiang, WANG Chao, et al. Data protection technology for information systems based on blockchain [ J ]. Journal of Command and Control, 2018, 4(3): 183-188
- [ 10 ] 田秀霞,陈希,田福粮.基于区块链的社区分布式电能安全交易平台方案[J].信息安全学报,2019,19(1):51-58  
TIAN Xiuxia, CHEN Xi, TIAN Fuliang. Community distributed power security transaction scheme based on blockchain [ J ]. Netinfo Security, 2019, 19(1): 51-58
- [ 11 ] 祝烈煌,董慧,沈蒙.区块链交易数据隐私保护机制[J].大数据,2018,4(1):46-56  
ZHU Liehuang, DONG Hui, SHEN Meng. Privacy protection mechanism for blockchain transaction data [ J ]. Big Data Research, 2018, 4(1): 46-56
- [ 12 ] 王继业,高灵超,董爱强,等.基于区块链的数据安全共享网络体系研究[J].计算机研究与发展,2017,54(4):742-749  
WANG Jiye, GAO Lingchao, DONG Aiqiang, et al. Blockchain based data security sharing network architecture research [ J ]. Journal of Computer Research and Development, 2017, 54(4): 742-749
- [ 13 ] 闫树,卿苏德,魏凯.区块链在数据流通中的应用[J].大数据,2018,4(1):3-12  
YAN Shu, QING Sude, WEI Kai. Application of blockchain in data circulation [ J ]. Big Data Research, 2018, 4(1): 3-12
- [ 14 ] 王玉娟,贾建华.“码”上扫京东 APP 食品区块链溯源信息提高食品安全透明度[J].条码与信息系统,2018(6):19-21  
WANG Yujuan, JIA Jianhua. Scanning Jingdong APP food block chain traceability information on code improves food safety transparency [ J ]. Bar Code and Information System, 2018 (6): 19-21
- [ 15 ] 郭珊珊.供应链的可信溯源查询在区块链上的实现[D].大连:大连海事大学,2017  
GUO Shanshan. Implementation of the supply chain's trusted traceability query on the blockchain [ D ]. Dalian: Dalian Maritime University, 2017
- [ 16 ] 杨云勇,马纪丰,胡川.安全 RFID 和区块链技术在瓶装酒防伪溯源中的应用研究[J].集成电路应用,2018

- (3):66-69  
YANG Yunyong, MA Jifeng, HU Chuan. Study on the application of safe RFID and block chain technology in the anti counterfeiting and traceability of bottled wine [J]. Application of IC, 2018(3):66-69
- [17] 刘晓云, 王晓春. “物联网+区块链”的农产品质量溯源体系研究[J]. 常州工学院学报, 2018, 31(5):60-65  
LIU Xiaoyun, WANG Xiaochun. Research on the traceability system of agricultural product quality based on “internet of things+blockchain” [J]. Journal of Changzhou Institute of Technology, 2018, 31(5):60-65
- [18] 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述[J]. 网络与信息安全学报, 2016, 2(11):11-20  
SHEN Xin, PEI Qingqi, LIU Xuefeng. Survey of block chain [J]. Chinese Journal of Network and Information Security, 2016, 2(11):11-20
- [19] 刘雪松. 点对点网络通信系统的设计与实现[D]. 长春: 吉林大学, 2010  
LIU Xuesong. Design and realization of a peer to peer net communication system [D]. Changchun: Jilin University, 2010
- [20] 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2018, 44(11):2011-2022  
YUAN Yong, NI Xiaochun, ZENG Shuai, et al. Blockchain consensus algorithms: the state of the art and future trends [J]. Acta Automatica Sinica, 2018, 44(11):2011-2022
- [21] King S, Nadal S. PPCoin: Peer-to-peer crypto-currency with proof-of-stake [EB\OL]. (2012-08-19) [2019-06-29]. <https://www.doc88.com/p-0788912122970.html>
- [22] 孙铁石. 如何做好学术论文的价值判断[J]. 长春理工大学学报(社会科学版), 2017, 30(6):139-142  
SUN Tieshi. How to judge the value of academic papers [J]. Journal of Changchun University of Science and Technology (Social Sciences Edition), 2017, 30(6):139-142
- [23] 韩璇, 刘亚敏. 区块链技术中的共识机制研究[J]. 信息网络安全, 2017(9):147-152  
HAN Xuan, LIU Yamin. Research on the consensus mechanisms of blockchain technology [J]. Netinfo Security, 2017(9):147-152
- [24] 陈宇翔, 张兆雷, 刘地军, 等. 区块链的税收智能合约设计[J]. 通信技术, 2018, 51(6):1384-1390  
CHEN Yuxiang, ZHANG Zhaolei, LIU Dijun, et al. Smart contract design for tax scenario based on block-chain [J]. Communications Technology, 2018, 51(6):1384-1390

## A blockchain-based academic paper review and traceability system

DING Yong<sup>1</sup> XIANG Hengkui<sup>1</sup> YUAN Fang<sup>2</sup> LUO Decun<sup>1</sup> LIU Lingang<sup>1</sup> ZOU Xiuqing<sup>1</sup> TANG Chenjun<sup>1</sup>

<sup>1</sup> School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004

<sup>2</sup> Communications Bureau of the Ministry of Foreign Affairs, Beijing 100016

**Abstract** In the era of mobile internet, it is more and more convenient to access professional knowledge and information, meanwhile, academic misconducts such as plagiarism and fraud are receiving increasing attention. With the emergence of digital currencies such as Bitcoin, the underlying blockchain technology also enters into people's sights. Based on the decentralization, trustworthiness and traceability of blockchain technology, this paper proposes a blockchain-based academic paper review and traceability system. While eliminating the high cost and security problems brought by the centralized system, the proposed system retrieves, records, and stores the academic papers with their reviewing and publishing processes, thus make the papers safe and traceable.

**Key words** blockchain; decentralization; paper review; trace back