

# 适用于数字版权保护交易的共识协议

汤小鹏, 薛涛

(西安工程大学 计算机科学学院, 陕西 西安 710048)

**摘要:**针对现有的数字版权保护交易都是在以 PoW、PoS 为基础的共识协议上进行的研究设计, 存在对资源消耗高、达成共识速度慢、效率低等问题。考虑到交易速度快、耗费成本低、交易量大等的特性, 该文在 DPoS 协议的基础上, 在节点被选为代理节点时, 通过节点交易频次和信用变化值来衡量节点的积极性, 进而提出了一种适用于数字版权保护交易的共识协议 T-DPoS。该协议采用节点状态作为补充, 降低错误节点当选的概率。在分布式网络上进行 8 个节点的竞争实验, 在每轮实验中进行 1 000 次程序的运行以保证实验的持续性, 证明积极性更高的节点更可能成为代理节点且错误节点当选概率能够控制在 1% 以内, 更适合数字版权保护交易系统。该技术可以在线上进行分布式部署完成数字版权保护交易。

**关键词:**区块链; 共识协议; DPoS; 数字版权; 分布式网络

**中图分类号:** TP399

**文献标识码:** A

**文章编号:** 1673-629X(2022)10-0108-06

doi:10.3969/j.issn.1673-629X.2022.10.018

## A Consensus Protocol for Digital Rights Protection Transaction

TANG Xiao-peng, XUE Tao

(School of Computer Science, Xi'an Polytechnic University, Xi'an 710048, China)

**Abstract:** The existing digital rights protection transactions are all researched and designed based on PoW and PoS-based consensus protocols. There are problems such as high resource consumption, slow consensus reached, and low efficiency. In view of the characteristics of fast transaction speed, low cost, large trading volume, etc, based on the DPoS protocol, we measure the enthusiasm of the node by the node transaction frequency and credit change value when the node is selected as the proxy node, and then propose a consensus protocol T-DPoS for digital rights protection transaction. This protocol uses node status as a supplement to reduce the probability of the wrong node being elected. The competition experiment of 8 nodes is carried out on the distributed network, and 1000 program runs are carried out in each round of experiment to ensure the continuity of the experiment. It is proved that a node with higher enthusiasm is more likely to become a proxy node and the probability of a wrong node can be controlled within 1%, which is more suitable for a digital rights protection transaction system. Such technology can be distributed online to complete digital rights protecting transactions.

**Key words:** Blockchain; consensus protocol; DPoS; digital rights; distributed network

## 0 引言

近年来,随着新媒体的迅猛发展,数字媒体信息呈现爆炸性增长。2020 年中国数字娱乐核心产业经济规模达 6 835.2 亿元,行业主要收入来源于用户付费和版权运营,新技术不加限制的滥用、内容传播途径的多样化、盗版行业实现全产业链的覆盖,造成盗版规模逐年上升,以网络文学为例,其遭受侵权的比例高达 42%。

数字版权交易规模随着行业的发展呈指数级增长,多元化的数字媒体如图片、音乐、视频等使得侵权

方式更多样化,更为复杂。2018 年 9 月蚂蚁链通过与杭州互联网法院联手打造区块链技术协助判案司法存证平台,以及国家版权中心在 2019 年 3 月与众多公司合作提出的 DCI 联盟体,表明数字版权交易可以与国家政府进行合作,在法律层面得到认可。传统数字版权保护交易系统过于依赖第三方机构,效率低、流程繁琐、成本高的问题变得越来越突出<sup>[1]</sup>,如何解决这些问题成为了行业的难点。区块链技术结合密码学算法、数字验证和分布式共识协议使得区块很难被篡改,它的另一个重要的特性就是其自身可以作为分布式存储

收稿日期:2021-09-16

修回日期:2022-01-18

基金项目:陕西省 2020 年技术创新引导专项(基金)计划(2020CGXNG-012)

作者简介:汤小鹏(1996-),男,硕士研究生,CCF 会员(18385G),通信作者,研究方向为区块链、共识协议、数字版权保护;薛涛,教授,硕士,博士,CCF 会员(27540M),研究方向为云计算、大数据和人工智能等。

数据库对数据进行存储<sup>[2]</sup>,保证了数据不会被删除。因为这些特性,其可以很好地应用在数字版权保护交易系统中。

国内很早就开始研究利用区块链技术对数字版权进行保护。2014 年,徐珉川提出将比特币中去中心化的特征应用到知识产权保护中<sup>[3]</sup>。文献[4]中同样在比特币的基础上提出一种数字版权保护模型。中国版权中心在 2015 年开始研究区块链技术在数字版权保护方面的研究,2019 年与国内多家头部互联网公司和机构发布 DCI 标准联盟链体系<sup>[5]</sup>。文献[6]中利用工作量证明共识协议 PoW (Proof of Work) 提出了一种基于区块链的数字作品 DCI 管控模型。迅雷公司采用能力权益授权共识 DPoA (Delegated Proof-of-Ability) + 实用拜占庭容错共识 PBFT (Practical Byzantine Fault Tolerance) 运用在其联盟链上从而解决版权保护问题<sup>[7-8]</sup>。

目前市面上运用比较成熟的都是采用基于 PoW 的共识协议,该协议虽然运行稳定,但是达成共识一致性的速度迟缓,不符合大规模的数字版权保护交易<sup>[9]</sup>。权益证明协议 PoS (Proof of Stake) 虽然降低了大量的算力竞争,但是创建时间越早,拥有股份越多的节点在后期会比其他节点更容易获取奖励,使得少部分节点处于垄断地位的问题没有得到解决,这并不利于系统的扩展<sup>[10]</sup>。商用公司往往采用的都是基于权益授权共识协议 DPoS (Delegated Proof of Stake)<sup>[11]</sup>,能够显著提高交易速度,同时也存在获得记账权奖励时只发放给代理节点,普通节点在投票时消耗一定的资源却获取不到奖励,造成投票参与度下降、中心化程度加剧的问题。

针对上述问题,该文提出一种适用于数字版权保护交易的共识协议,简称 T-DPoS (Transaction-Delegated Proof of Stake)。该共识协议通过各节点的状态和奖励制度,提高节点参与投票的积极性,保持交易系统中节点投票的活跃度,降低错误节点当选的概率,并通过各节点的交易频次,判断出节点参与的积极性,保证积极性高的节点更容易被选取成为代理节点,在保证安全的基础上能够更好地控制交易速度,同时能够保证各方的利益使其能够更好地适用于数字版权保护交易系统。

## 1 相关工作

### 1.1 PoW 共识协议

早期的区块链网络中,都是以 PoW 共识协议作为基础,其中比较经典的是以比特币为首的加密货币。在此共识协议中,为了达成一致性要求,每个节点必须为新的区块找到随机数,由当前区块的随机数及先前

的散列块与新块中的事务一起通过散列函数算法<sup>[12]</sup>(如 SHA256)得到在一定区间内的结果,当节点找到这个随机数之后,生成一个区块,通过广播到整个分布式网络中,只有被确定为链中最后一个区块的时候才能够被确认<sup>[13]</sup>。为了保证区块出块速度稳定,会随网络变动调整寻找随机数的难度值,也就意味着块确定的速度并不是很快。如比特币大概是每 10 分钟出一个块,块的大小为 1 M,每秒能够处理 6.6 笔交易。节点取得对区块记账权的概率与设备的计算能力成正比关系,具体如下:

$$p_i = \frac{X_i}{\sum_{j=1}^n X_j} \quad (1)$$

其中,  $X_i$  代表的是该节点的算力,其与设备的性能有关。当设备的算力越强,寻到随机数的概率也就越大,在寻找随机数的同时会因为设备之间竞争寻找随机数而消耗大量的资源<sup>[14]</sup>。

### 1.2 PoS 共识协议

PoS 共识协议与 PoW 的不同之处在于,其不是在同等的条件下争夺区块的记账权,而是在创建一个新的区块时,节点获得区块记账权的概率与之所持有的代币和天数成反比。相对于 PoW 来说,每个想获得区块记账权的用户都是用自身条件而非设备解决问题。在有些基于 PoS 的共识协议改进协议上<sup>[15]</sup>,块的产生已经舍弃了算力这种方式,而是通过所持有的股份决定。这在一定程度上避免了挖矿所带来的资源浪费。用户获得的区块打包权概率计算公式如下:

$$p_i = \frac{S_i}{\sum_{j=1}^n S_j} \quad (2)$$

$S_i$  代表的是用户所拥有的期权,随着股份的增多用户获得的打包权的概率也会随之增大。区块链进一步地发展壮大,会造成节点的垄断,新节点相比于旧节点获得打包权的概率会小很多,这不符合区块链公平性发展的宗旨。在处理交易的速度上,相较于 PoW 缩短了各个节点之间达成的共识时间,效率得到了进一步提升。

### 1.3 DPoS 共识协议

DPoS 共识协议相较于 PoS、PoW 协议更加有效、快速、分散。如同现代集团式决策管理层,由持有者选出一些代理节点,选出的方式也更加民主与公平<sup>[16]</sup>,这些代理节点可以调整网络的参数、区块间距、交易规模,之后会轮流地生成区块,收集一段时间内网络上未确定的交易。如果一个代理节点有恶意的行为,或者不正确使用权力,将会在后续中被普通节点投票剔除<sup>[17]</sup>,再次选举新的节点成为代理节点。通过这种选择代理节点的做法,大大减少了参与验证和记账的节

点数量,缩短了达成共识的时间,从而使得效率得以提高。三种协议的比较详情见表 1。

表 1 三种共识协议对比

	PoW	PoS	DPoS
获得打包权方式	Hash 函数	股权	节点选举
新块产生速度	慢	较快	快
交易确认速度	慢	较快	快
设备需求	高	较低	低
能耗	高	较低	低

## 2 设计思路

### 2.1 T-DPoS 共识协议设计思想

T-DPoS 共识协议在 DPoS 协议的基础上加入节点状态的判别来降低错误节点当选的概率和节点奖励机制以解决 DPoS 投票积极性不高的问题,同时加入交易频次,优化代理节点的选取使之更加贴合数字版权保护交易系统。设计选取出的代理节点有以下几个特质:(1)网络保持同步状态,诚实节点之间保持利益的相关性,节点之间会进行投票,平衡各方的利益。(2)利益相关节点保持长时间的在线,如果长时间离线会影响信用值。(3)设计一个兜底节点,可以保证系统安全运行。(4)代理节点需要在交易系统平台上上交一定的费用,用来防止这些代理点恶意或消极的进行版权检测,当交易处理完成后,根据奖励分配原则获得部分奖励。

其具体设计机制是在数字版权保护交易系统中,根据 T-DPoS 共识协议选择代理节点,共识程度越高,被选为代理节点的可能性越高。共识程度由该节点的交易频次、信用变化值和节点之间的投票值来决定。交易频次是指一段时间内(两次投票时间)系统统计该节点进行了多少次版权交易。信用变化值指的是该节点能够认真完成交易任务,即该节点积极参与代理节点的竞争并被选择为代理节点,获得的信用奖励,反之,节点如果长时间内未被选为代理节点,会导致信用消耗,被认为是消极应对或有恶意行为。投票值是由节点之间互相投票,节点获得的票数决定的。具体算法如下所示:

$$G = \alpha F + 0.6 \Delta C_{\text{credit}} + \beta V \quad (3)$$

$$V = \sqrt{S} \quad (4)$$

其中,  $F$  代表交易的频次,  $\Delta C_{\text{credit}}$  代表信用变化值,衡量节点参与交易系统的积极性,  $V$  代表各个节点的投票值,投票值与各节点持有的股份成正比。该文限制节点投票的数量为 10,使用公式 4 降低投票的权重,使得投票的比重在共识中处于合理的范围。其中  $\alpha + \beta = 1$ ,为了鼓励节点能够参与系统交易,实验中取

$\alpha = 0.6, \beta = 0.4$ 。信用变化值计算公式为:

$$\Delta C_{\text{credit}} = \Delta C_+ - \Delta C_- \quad (5)$$

其中,  $\Delta C_-$  表示节点的信用损耗,  $\Delta C_+$  表示节点可获得的信用增益,具体表达式如下:

$$\Delta C_- = \begin{cases} t/T, & t > T \\ 0, & t \leq T \end{cases} \quad (6)$$

$$\Delta C_+ = M \quad (7)$$

其中,  $t$  代表两次投票的间隔时间,  $T$  代表交易的周期,两次投票的间隔时间越长,信用值损耗越大。文中交易时间取值为 3 个区块产生的时间,节点两次投票时间的间隔过长,系统自动判定为消极应对交易服务。在信用奖励的公式(7)中,  $M$  代表节点积极参与系统交易且产生了有效区块,选出合适的代理节点获得的信用奖励,文中取常量值为 1,鼓励节点积极投票。

### 2.2 T-DPoS 共识协议工作流程

用户上传作品,通过版权中心标准判断是否符合原创作品。共识协议首先根据节点状态进行投票,用奖励分配来降低系统中错误状态节点当选的概率,根据节点的交易频次、交易的信用变化值选举出代理节点。节点之间通过分布式网络进行交易的确证,完成交易并获得奖励。其流程如图 1 所示。

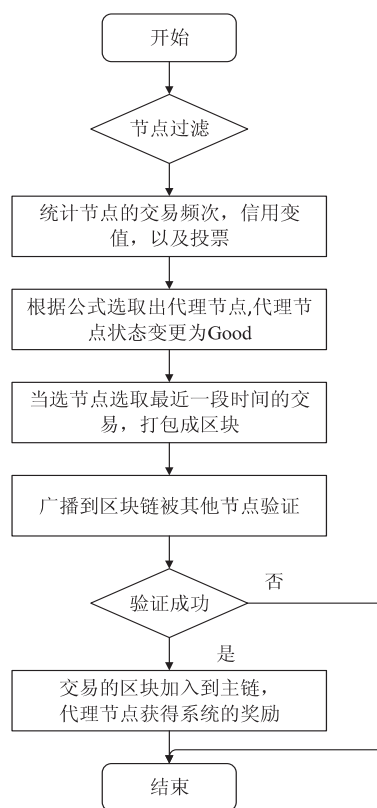


图 1 T-DPoS 共识协议流程

### 2.3 节点状态变更流程与收益分配

节点状态的变更是 T-DPoS 共识协议中重要的一环,将其与收益分配结合可以提高节点参与投票的积极性,它与代理节点产生区块的数量及有效性有关。



节点分为三种状态,即普通状态、良好状态和错误状态。其状态转换关系如图 2 所示。

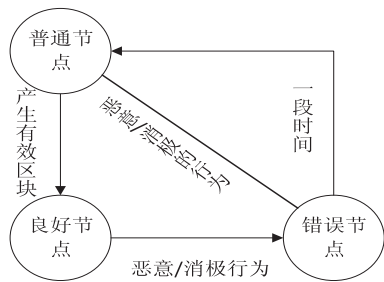


图 2 节点状态转换

节点的初始状态是普通状态,当节点成为代理节点之后能够产生被其他节点认可的区块且数值超过一定的数量值(文中取值为 3),状态升级为良好状态,代理节点产生无效区块或者有恶意行为时,节点会被定义为错误状态。当节点之间投票时,由于节点有网络保持同步状态的性质,能够知道彼此的状态,投票的时候可以依此来进行判断,降低恶意节点当选的概率。当节点被判定为错误状态之后,需要经过一段时间才可以恢复到正常状态。

在收益分配中,当节点当选为代理节点时,节点会按照股权的多少进行收益的分配,文中采用节点的投票值来模拟股权。收益主要由记账权收益获得,记账权收益为申请版权保护方在区块产生时间内缴纳的费用与这段时间内产生区块的比值,其中代理节点将获得块中交易的 10% 作为奖励,其余收益按照各个节点前期投票的比例进行利益的分配。收益分配是为了鼓励节点成为代理节点,同时鼓励节点投票使得系统的活跃度上升,提高节点参与交易的积极性。

### 3 实验分析

#### 3.1 实验环境

该文基于 DPoS 共识机制实现代理节点的选取,建立 8 个分布式网络节点,选取 3 个代理节点,每个节点拥有 10 票的投票权。实验环境操作系统为 Centos7 (64 位),处理器为 CPU-Intel(R) Xeon(R) CPU E5-2620(主频是 2.00 GHz,6 GB),编程语言使用 Go 语言,Geth 版本为 1.10.4-unstable。

#### 3.2 实验结果与分析

为了验证该方法的有效性,进行了 4 次实验验证不同属性对选取代理节点的影响。实验一与实验二基于交易频次和信用变化值进行对比论证,实验三与实验四基于节点状态进行对比论证,每轮实验基于 1 000 次的程序运行。

表 2 为实验一与实验二各个节点的属性值,实验一只考虑节点的交易频次,通过比较各个节点当选为代理节点次数,得出交易频次属性对节点成为代理节

点所带来的影响。各个节点的属性值见表 2,其中信用增益为第二次实验对应节点的属性变化。

表 2 实验一与实验二节点属性

节点	交易频次	信用增益
1	4	1
2	4	0
3	4	1
4	5	0
5	5	1
6	5	0
7	8	0
8	8	0

可以看出:节点 1、2、3 交易频次较少,4、5 节点适当增加,7、8 节点交易频次较多,代表积极性较高的节点。实验二中因为节点 1、3、5 积极参与交易系统的投票,信用增益分别增加 1,各个节点的属性值见表 3。

实验程序运行 1 000 次,实验一与实验二中各节点当选为代理节点的次数对比结果如图 3 所示。

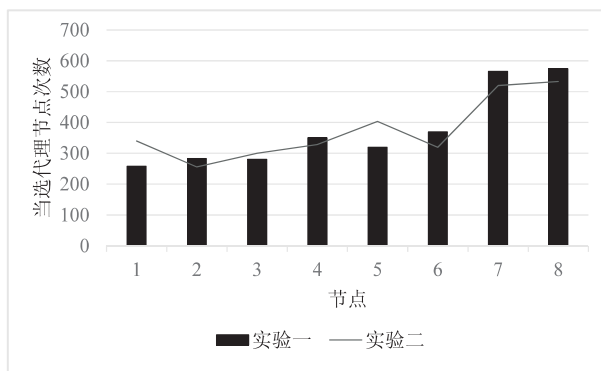


图 3 实验一与实验二节点当选次数对比

第 1 次实验由系统随机投票,投票相对均匀,不考虑信用增益与损耗,节点被选为代理节点主要是由交易的频次决定。由图 3 可以看出,节点 7、8 获得代理节点次数较多,这是因为在系统中交易的频次高,表明交易频繁节点参与积极性高,当选代理节点的概率越大。交易频次接近的,当选为代理节点次数也接近。实验二相较于实验一,1、3、5 节点有较为明显的变化,提高节点的增益值,可以提高节点被选中的概率。相较于没有信用增值的节点,较实验一中被选为代理节点次数降低。

当其中一个当选节点有恶意行为或产生无效区块,将被系统判别为错误节点。在实验三中,考虑投票值对节点当选为代理节点的影响,未加入节点状态因素的影响。由系统产生第一轮投票,各节点属性见表 3。

实验四中共识协议根据加入节点状态因素,交易系统进行了节点的第二轮投票,投票值发生了变化,这

是因为网络呈彼此可见状态,以及系统奖励机制的作用,各节点属性见表 4。

表 3 实验三节点属性

节点	交易频次	信用增益	投票值	节点状态
1	4	0	13	普通
2	4	0	8	普通
3	0	0	12	异常
4	4	0	8	普通
5	4	0	10	普通
6	4	0	9	普通
7	4	0	11	普通
8	4	0	9	普通

表 4 实验四节点属性

节点	交易频次	信用增益	投票值	节点状态
1	4	0	13	普通
2	4	0	11	普通
3	0	0	1	异常
4	4	0	10	普通
5	4	0	14	普通
6	4	0	10	普通
7	4	0	11	普通
8	4	0	11	普通

程序同样运行 1 000 次,实验三与实验四中各参选节点竞选成为代理节点的次数对比结果如图 4 所示。

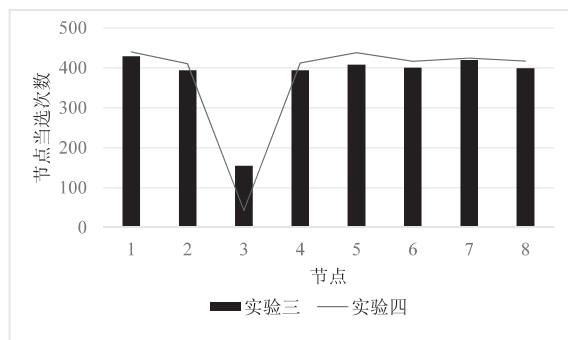


图 4 实验三与实验四节点当选次数对比

图 4 为两轮投票的实验数据对比,在第一轮投票中没有考虑节点状态的因素,投票分布较为均匀,实验中各节点被选为代理节点的概率接近,因为节点 3 消极应对交易系统,没有达到考核量的标准所以节点被系统标注为错误节点,相对于其他普通节点,错误节点当选的概率较低。二轮投票中,考虑到节点状态以及奖励机制的作用,节点投票会更倾向于普通节点,相应的错误节点获取的票数降低。相较于实验三,错误节点当选为代理节点的次数进一步降低,当选概率不足 1%。

达成共识耗费的时间决定了交易花费的时间,图

5 为 25 次共识程序的运行时间变化。

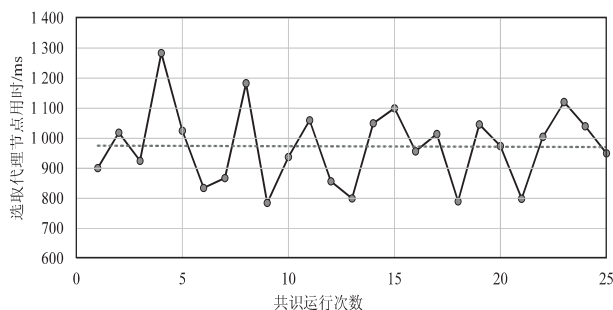


图 5 共识时间统计

由图 5 可以看出,在相同的网络条件下,交易时间在 1 000 ms 上下波动,相较于 PoW 和 PoS 共识协议的交易时间提升到秒级,可以提高交易的效率,能够更好地应用到交易系统中。

## 4 结束语

在 DPoS 共识协议的基础上,结合数字版权保护交易系统的需求,考虑节点参与积极性,提出一种适用于数字版权保护交易的 T-DPoS 共识机制。利用分布式网络,创造 8 个节点模拟选举 3 个代理节点。实验表明,积极参与交易的节点更容易成为代理节点,同时,增加信用增益、降低信用损耗也能够提升成为代理节点的概率。选举节点的时间相较于其他的共识协议算法有明显的缩短,更符合交易系统的需求。后续会

考虑奖励分配对代理节点产生带来的影响,以及错误节点如何被剔除不参与代理节点的选取,并将其应用于数字版权保护的的交易系统中。

#### 参考文献:

- [1] 库文妍,姚海龙. 浅谈区块链技术在数字版权管理领域的应用——价值、现状与问题[J]. 传播与版权, 2020(5):112-114.
  - [2] MUZAMMAL M, QU Qiang, NASRULIN B. Renovating blockchain with distributed databases; an open source system[J]. Future Generation Computer Systems, 2019, 90(2):105-117.
  - [3] 徐珉川. 知识产权的“去中心化”——比特币与登记制度[J]. 科技与法律, 2014(3):474-497.
  - [4] 韩 锋, 顾 颖, 贾红宇, 等. 一种基于比特币区块链的知识产权众筹模式[J]. 清华金融评论, 2014(6):98-101.
  - [5] 赖利娜, 李永明. 区块链技术下数字版权保护的机遇、挑战与发展路径[J]. 法治研究, 2020(4):127-135.
  - [6] 李 悦, 黄俊钦, 王瑞锦. 基于区块链的数字作品 DCI 管控模型[J]. 计算机应用, 2017, 37(11):3281-3287.
  - [7] 郑小峰. 迅雷链基于智能硬件的 DPoA 共识机制介绍[EB/OL]. [2018-12-06]. <https://juejin.cn/post/6844903732325384200>.
  - [8] SIK H H, YOUNG S D. A study on scalable PBFT consensus algorithm based on blockchain cluster[J]. The Journal of The Institute of Internet, Broadcasting and Communication, 2020, 20(2):45-53.
  - [9] 程 瑶, 高丽芬, 胡全贵. 区块链共识机制之 POW 算法[J]. 数字通信世界, 2019(3):81.
  - [10] NGUYEN C T, HOANG D T, NGUYEN D N, et al. Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities[J]. IEEE Access, 2019(7):85727-85745.
  - [11] YANG F, ZHOU W, WU Q, et al. Delegated proof of stake with downgrade; a secure and efficient blockchain consensus algorithm with downgrade mechanism[J]. IEEE Access, 2019(7):118541-118555.
  - [12] YANG Yijun, CHEN Fei, ZHANG Xiaomei, et al. Research on the hash function structures and its application[J]. Wireless Personal Communications, 2017, 94(4):2969-2985.
  - [13] 刘海房, 吴雨芯. 比特币系统综述[J]. 现代计算机, 2020(19):45-51.
  - [14] ZHANG Cong. Power consumption perception pow consensus mechanism for block chain; CN, WO2018032371[P]. 2018-02-22.
  - [15] SONG Rui, SONG Yubo, LIU Ziming, et al. GaiaWorld: a novel blockchain system based on competitive PoS consensus mechanism[J]. Computers, Materials & Continua, 2019, 60(3):973-987.
  - [16] 黄嘉成, 许新华, 王世纯. 委托权益证明共识机制的改进方案[J]. 计算机应用, 2019, 39(7):2162-2167.
  - [17] ZHENG Z, XIE S, DAI H, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]//Proceedings of the 2017 IEEE international congress on big data (BigData congress). Honolulu: IEEE, 2017.
- +++++
- (上接第 107 页)
- [8] LI H, TIAN H, ZHANG F, et al. Blockchain-based searchable symmetric encryption scheme[J]. Computers & Electrical Engineering, 2019, 73:32-45.
  - [9] 牛淑芬, 谢亚亚, 杨平平, 等. 区块链上基于云辅助的属性基可搜索加密方案[J]. 计算机研究与发展, 2021, 58(4):811-821.
  - [10] 王小云, 于红波. SM3 密码杂凑算法[J]. 信息安全研究, 2016, 2(11):983-994.
  - [11] 吕述望, 苏波展, 王 鹏, 等. SM4 分组密码算法综述[J]. 信息安全研究, 2016, 2(11):995-1007.
  - [12] CASH D, JAEGER J, JARECKI S, et al. Dynamic searchable encryption in very-large databases; data structures and implementation[C]//Network & distributed system security symposium. Berlin: Springer, 2014:23-26.
  - [13] 袁 峰, 程朝辉. SM9 标识密码算法综述[J]. 信息安全研究, 2016, 2(11):1008-1027.
  - [14] 闫玺玺, 原笑含, 汤永利, 等. 基于区块链且支持验证的属性基搜索加密方案[J]. 通信学报, 2020, 41(2):187-198.
  - [15] 杜瑞忠, 谭艾伦, 田俊峰. 基于区块链的公钥可搜索加密方案[J]. 通信学报, 2020, 41(4):114-122.
  - [16] YAN X, YUAN X, YE Q, et al. Blockchain-based searchable encryption scheme with fair payment[J]. IEEE Access, 2020, 8:109687-109706.