基于贡献值和难度值的高可靠性区块链共识机制

何泾沙[1),2)] 张 琨[1)] 薛瑞昕[1)] 朱娜斐[1)] 贺 鹏[2)]
宋洪宇[1)] 杜伟东[1)] 甘 宇[1)]

[1)](北京工业大学信息学部 北京 100124)

[2)](三峡大学计算机与信息学院 湖北 宜昌 443002)

摘 要 基于贡献值证明(PoC)的区块链共识机制是面向知识产权保护与交易应用场景提出的一种区块链共识机制,通过计算节点用户的贡献值,由贡献值最大的节点获得新区块的记账权.然而,由于 PoC 会造成记账节点具有很强的确定性,一旦该节点未能正常完成记账出块,网络中其它节点将始终保持在挂起等待状态,系统将陷于停滞状态,无法继续运行.为了使 PoC 区块链共识机制能够适用于公有链应用场景,本文提出基于贡献值和难度值(PoC+PoW)的区块链共识机制,使选择新区块记账权的节点具备一定的不确定性,能够有效解决 PoC 共识机制中存在的系统运行挂起缺陷.在 PoC+PoW 共识机制中,节点在工作量证明(PoW)竞争中所对应数学难题的难度值根据节点的贡献值(PoC)进行动态确定,是一种对单纯基于 PoC 共识机制的灾备方案,以确保系统运行的可靠性.本文提出的 PoC+PoW 方案根据节点的贡献值排名为节点分配相应的 PoW 难度值,节点再通过 PoW 共识机制竞争记账权.引入 PoW 后的共识机制最大程度地尊重 PoC 贡献值排名,使节点的记账出块率与其贡献值成高度正比,在系统运行层面则保证记账出块率达到或无限趋近 100%,有效解决 PoC 带来的系统运行挂起问题.本文从节点贡献值排名、相邻贡献值节点间值差以及分组方式三个角度设计 PoW 难度值分配算法,并通过实验验证难度值分配算法的合理性和有效性.同时,通过实验与传统 PoC 共识机制在记账出块时延方面进行对比分析,进一步验证了 PoC+PoW 方案的优越性和可行性.

关键词 区块链;共识机制;贡献值;贡献值证明;难度值;工作量证明

中图法分类号 TP311 **DOI 号** 10.11897/SP.J.1016.2021.00162

A Highly Reliable Consensus Mechanism for Blockchain Based on Contribution and Difficulty Values

HE Jing-Sha[1),2)] ZHANG Kun[1)] XUE Rui-Xin[1)] ZHU Na-Fei[1)] HE Peng[2)]
SONG Hong-Yu[1)] DU Wei-Dong[1)] GAN Yu[1)]

[1)](*Faculty of Information Technology, Beijing University of Technology, Beijing* 100124)

[2)](*College of Computer and Information Technology, China Three Gorges University, Yichang, Hubei* 443002)

Abstract A consensus mechanism for blockchain based on proof of contribution (PoC) is a kind of consensus mechanism that is suitable for the application scenarios of intellectual property protection and transaction. In the PoC mechanism, the contribution values of user nodes are calculated periodically and the node with the largest contribution value will assume the right for the construction of a new block. However, the PoC consensus mechanism has the problem that the node that constructs the new block in the current round exhibits the property of strong

收稿日期:2019-11-29;在线发布日期:2020-05-12.本课题得到国家重点研发计划课题(2019QY(Y)0601)资助.**何泾沙**,博士,教授,主要研究领域为网络安全、区块链技术、数字取证.E-mail:jhe@bjut.edu.cn.**张 琨**,硕士研究生,主要研究方向为区块链技术及共识机制.**薛瑞昕**,硕士研究生,主要研究方向为区块链技术与应用、区块链共识机制设计.**朱娜斐**(通信作者),博士,副教授,主要研究方向为隐私保护、信息安全、区块链技术.E-mail:znf@bjut.edu.cn.**贺 鹏**(通信作者),博士,教授,主要研究领域为基于网络时间同步的传输协议和信息安全.E-mail:hpeng@ctgu.edu.cn.**宋洪宇**,硕士研究生,主要研究方向为区块链系统与共识机制设计.**杜伟东**,硕士研究生,主要研究方向为区块链技术.**甘 宇**,硕士研究生,主要研究方向为区块链技术.

certainty. If the node that is supposed to construct the new block in the current round fails to do so, all the other nodes will remain in the waiting state and the system will hang and execution can no longer continue. To make the PoC blockchain consensus mechanism applicable to the public chain scenario, this paper proposes a new consensus mechanism based on the contribution value as well as on the difficulty value in the proof of work consensus mechanism (PoC+PoW). In the PoC+PoW consensus mechanism, some uncertainty is added into the process of determining the right for the construction of a new block to overcome the shortcomings of the original PoC consensus mechanism. In PoC+PoW, the difficulty values of the mathematical problem that participating nodes try to solve in the PoW competition is dynamically determined according to the PoC values of the nodes. The proposed mechanism can thus be viewed as a disaster recovery scheme for the PoC consensus mechanism to ensure the reliability of the system operation. The proposed PoC+PoW consensus mechanism would allocate a corresponding PoW difficulty value to a node according to the ranking of the contribution value of the node. All nodes then compete for the right for bookkeeping and block construction through the PoW consensus mechanism. The new consensus mechanism that incorporates PoW would still fully respect the ranking of the contribution values from PoC to ensure that the probability of constructing a new block by a node is highly proportional to its ranking among all the contribution values. As far as system operation is concerned, the probability of block construction can be guaranteed to reach or approach infinitely to 100%, which should effectively solve the system hanging problem existing in PoC-based systems. This paper will present the design of an algorithm for the allocation of the PoW difficulty values from three aspects: the ranking of the contribution values, the difference between adjacent contribution values and the grouping method, and will verify the rationality and effectiveness of the proposed allocation algorithm through experiment. In addition, a comparison between the new PoC+PoW consensus mechanism and the traditional PoC consensus mechanism in terms of the efficiency of block construction further verifies the superiority and the feasibility of the proposed PoC+PoW consensus mechanism.

Keywords　blockchain; consensus mechanism; contribution value; Proof of Contribution; difficulty value; Proof of Work

1　引　言

区块链技术[1-3]具有去中心化、数据时序、不可篡改、可追溯、集体维护、可编程和安全可信等特点[4].区块链中的数据存储按照时间戳的顺序不断更新,可以使任何记录在内的数据或活动都拥有不可篡改的跟踪记录,并且无需依赖可信第三方的帮助①.区块链是比特币[5]的底层技术,是一个集成了密码学、分布式存储、点对点网络[6]等技术及共识机制的综合性技术解决方案[7].在比特币区块链中,每一个节点都维护一部相同的账本,所有交易都需要对全网进行广播,并经过节点验证通过后,方可写入账本.区块链账本因其数据的分布式记录与存储、可追溯、不可篡改等特点具有去中心化的特性,并在系统节点之间建立起了全新的信任机制,使系统能够在不依赖任何中心化组织的情况下运行,从而实现系统的自治性和公平性.

共识机制是区块链系统的灵魂和法律,承担着维系区块链系统正常运转的核心功能.有效的共识机制可提升系统性能、促进区块链技术得到广泛应用[8-9].在区块链中,每一个节点都维护着一部相同的账本,账本的记账权分配不依赖中心化,而是根据共识机制决定点与点的交易在时间十分相近情况下规则性的排序.到目前为止,已经发展出很多不同类型的区块链共识机制.

工作量证明(Proof of Work,PoW)[10]作为已知

① 中国保护知识产权网. 区块链技术在知识产权领域的应用. 2017.10.12. http://ipr.mofcom.gov.cn/article/gjxw/gfgd/201710/1911897.html

的第一个区块链共识机制，应用于比特币以及以太坊[①②]，来解决谁是大多数的问题. PoW 以及根据经济学原理制定的激励机制能够吸引更多的节点参与，成就了以比特币为代表的加密货币应用迅速发展，网络规模迅速扩大，在很大程度上可以实现相对公平. 然而，PoC 共识机制具有高能耗、违背环保理念的缺陷，矿池概念也会导致算力趋于中心化，并且随着出块奖励的逐步减少，矿工挖矿积极性降低，算力也会大幅下降，由此导致的比特币网络安全问题令人堪忧[11]. 由于 PoW 具有以上的缺陷，针对加密货币又提出了许多新的共识机制，其中股权证明机制(Proof of Stake，PoS)[12]通过充分论证与实践被认为具有可行性. PoS 共识机制没有挖矿过程，在创世区块内就写明股权分配比例，之后通过转让、交易的方式逐渐分散给用户，可通过发放利息的方式新增货币，对出块节点进行奖励. PoS 共识机制规定拥有币龄越高的节点就拥有越高的记账权. 简单来说，就是用户节点拥有越多的币，并且拥有币的时间越长，获得记账权的概率也就越大. 然而，由于 PoS 共识机制要求每一个节点都参与竞争，对网络吞吐量要求较高. 加密货币的另一种共识机制，即授权股权证明(Delegated Proof of Stake，DPoS)[③]，选取少部分节点作为代表进行记账，可以进一步降低能耗，并且确认速度更快. 然而，PoS 共识机制存在着投票积极性低这一明显不足，90%以上的节点从未参与投票，并且不能有效阻止破坏性节点，因此带来网络安全隐患.

区块链共识算法经过了不断创新与改进，从 PoW 到 PoS 再到 DPoS，可以说是共识机制早期发展的一条主线. 这三种共识机制各有优劣，比如 PoW 具有完整的数学证明，理论上来说最安全，实现相对简单，但在能源消耗、出块时间、交易容量方面存在很大不足，PoS 则存在安全风险更大、选举节点时网络流量压力很大以及“富者愈富，贫者愈贫”等问题，而 DPoS 由于缩小了选举节点数量而降低了网络压力，但却因此带来去中心化程度降低而备受争议[13].

根据对现有国内外研究背景分析，数字知识产权保护与区块链技术作为近年逐渐兴起的技术，应用前景十分广阔、应用价值十分明显. 利用区块链技术去中心化、可追溯、不可篡改等特性可以在知识产权的产出、确权、交易等多个环节进行准确记录. 区块链系统中用户产出知识产权后向系统上传自己的作品. 区块链系统对知识产权进行预先确权后，一旦发生知识产权侵权纠纷，用户便可以利用存储在区块链中的数据证明对该作品的所有权，达到维护自身合法权益的目的.

在区块链对知识产权对保护方面，国内外不乏优秀的企业项目案例. 德国初创企业艾斯克瑞博(Ascribe)在 2015 年通过利用区块链的时间戳技术，对知识产权进行时间标记并且为艺术作品乃至其它数字媒介创建可持续所有权结构，为艺术家提供艺术作品的登记、注册、交易服务[④]. 2016 年，美国技术公司布洛凯(Blockai)进行区块链版权服务运营项目，通过在区块链上记录永久有效的版权来方便艺术家、摄影师等内容创作者进行作品版权登记、保护艺术创作[⑤]. 2016 年，Eleks 实验室考虑采用面向作品的方法来使用区块链技术，它为客户提供了一种安全传输机密文件的方法. 它使用以太坊区块链作为主干，并使用智能合约[⑥]. 2017 年 8 月，欧洲著名知识产权咨询公司瓦力(Valea AB)撰文从设计区块链技术的专利、商标申请数量，以及区块链对时间戳、产品认证、智能合约、知识产权审查机构五个方面分析了当前区块链技术对知识产权行业的影响[⑦]，我国国内创业团队“原本”是基于区块链技术的版权认证和交易平台. 2016 年，原本将作品和版权信息的加密验证永久记录在区块链上，为作品提供免费、可靠的版权认证，对接线下公证处和律所服务，提供一站式服务.

区块链应用与数字化知识产权保护方面也成为近年来的研究热点，然而国内外的学术研究非常有限. Watanabe 等人[14]提出利用区块链和智能合约

① Buterin V, Wiederhold B, Riva G, et al. A next-generation smart contract and decentralized application platform. 2015-11-12. https://github.com/ethereum/wiki/wiki/White-Paper

② Wood G. A formal specification of Ethereum, a programmable Blockchain. 2018-11-12. https://ethereum.github.io/yellowpaper/paper.pdf

③ Bitshares. Delegated proof of stake. http://docs.bitshares.org/bitshares/dpos.html

④ Stan H. How ascribe uses Bitcoin tech to help underserved artists. 2017. https://www.coindesk.com/ascribe-bitcoin-tech-underserved-artists

⑤ Pete R. Blockai raises 547k for Blockchain digital rights platform. 2017. https://www.coindesk.com/blockai-raises-547k-to-relaunch-as-blockchain-digital-rights-platform

⑥ Eleks Labs. Secure document transfer built on top of Blockchain technologies. https://labs.eleks.com/2016/10/secure-document-transfer-built-top-blockchain-technologies.html

⑦ Valea AB. Blockchain technology expected to strongly impact the IP industry. 2017. https://www.lexology.com/library/detail.aspx?g=a1461135-598b-4c3c-811c-73ac70c3f67b

的概念来扩展区块链的应用领域,即智能合约达到预设合同条件时被相应执行. Kishigami 等人[15]提出了一种用于改变传统数字版权管理模式的基于区块链技术的内容分发系统. Liu[16]提出了一种基于区块链的三层知识产权注册服务平台,其中底层是区块链网络,中间层通过区块链共识机制构建知识产权服务逻辑,顶层是知识产权业务模块. Tsai 等人[17]研究了中国微电影/短视频的知识产权保护问题,借助区块链取存储观看记录、交易等信息,但主要集中在加密算法与框架说明上,并未涉及共识机制. Ajay 等人[18]提出用一个公共的分布式的分类账本代替文书工作的需要,记录并验证平台内完成的每笔交易,主要采用基于工作量证明的共识机制确保公共账本的完整性.

从以上知识产权结合区块链的企业应用和研究成果来看,数字化知识产权保护与区块链和共识机制结合的发展仍然存在广阔的空间.

首先,现有的应用于知识产权的区块链共识机制仍然以联盟链形式为主. 应用区块链对数字化知识产权进行保护的形式,目前多以联合数据保全平台、司法鉴定中心、第三方平台等为主要参与者,这样的区块链化的知识产权保护系统仍然存在不透明的现象,兼具中心化特征,对于数字知识产权的保护仍无法完全摆脱中心化所带来的信任问题[19].

其次,现有的主流共识机制在“知识产权保护”这一应用场景下的短板也较为突出. 其中,PoW 要求的高算力造成事实上的不必要资源浪费,既不环保也不经济,对知识产权保护无需通过采用 PoW 这类高耗能的共识机制来支持. 同时,PoS 权益证明共识机制虽然能够降低达成共识所需时间,但仍然需要依赖虚拟货币等资产,本质上仍需在网络中进行节点挖矿运算,且无法完全摆脱中心化的风险. 此外,目前学术研究大多集中在讨论区块链技术在知识产权保护应用中的优势,缺乏对区块链技术的特性与知识产权应用需求之间的矛盾的分析,将知识产权保护作为出发点的共识机制屈指可数,没有与知识产权应用场景形成很好的吻合.

再次,随着区块链技术的发展,形式单一的“发币”激励机制已不能满足区块链在实际应用场景中的要求. 以加密货币为主的区块链系统设置的激励机制目的是激励用户参与,通过更多用户参与区块链维护来提高系统的安全性[20]. 比特币以“发币”作为主要激励机制,通过虚拟货币较高的变现价值吸引了大量的用户参与,虽然提高了区块链网络的活跃度,但也间接造成了以“挖币”为目的的恶意算力竞争[21],背离了区块链技术去中心化的本意与初衷. 而 PoS 和 DPoS 等共识机制对数字货币资产依然有较高的依赖,无法完全契合“数字化知识产权保护”的应用场景. 为了设计更加符合实际应用场景的区块链共识机制,在知识产权保护应用中使用户关注点回归到对自身知识产权作品合法权益进行保护这一根本需求上,以期引导用户正确、积极地使用区块链,就需要设计新的结合实际应用场景,且非“币”形式的共识机制.

针对现有共识机制在“数字知识产权的保护”应用场景下的不足,提出了一种基于贡献值证明(Proof of Contribution, PoC)[22]的区块链共识机制. 在基于 PoC 的区块链系统中,每一轮竞争记账权都以参与节点对系统的贡献大小作为确定记账权的依据. 系统通过对节点的贡献值大小进行排序,将本轮的记账权赋给贡献值最大的节点. PoC 共识机制适用于以公有链形式构建的区块链系统,是一种非“币”形式而是基于节点贡献值累计与排序作为确定记账权的区块链共识机制. 因此该共识机制不仅可以应用于“数字知识产权保护”的应用场景之中,而且对于依赖用户(客户)实际参与行为以及用各种方式贡献而非“币”制运行的应用系统都适用.

然而,区块链系统中的参与节点通常无法保证持续在线的稳定性,受节点及网络环境各种因素的影响,会出现贡献值最大的节点在需要记账时下线或通信不畅等突发情况,从而导致系统无法继续运转. 大量的实验表明,基于 PoC 的区块链共识机制存在这方面的缺陷. 首先,受各种移动互联网环境因素的影响,贡献值最大的节点作为记账节点可能会无法正常记账出块,因此,需要有一个“候补记账节点”的选举方案,作为一个灾备方案来应对此类情况的发生. 此外,将贡献值作为区块链系统节点记账的唯一依据,在一定程度上也不利于鼓励其它节点的积极参与. 在贡献值最大的节点还未能完成记账的情况下,让贡献值接近的其它节点也有机会获得记账权,可以在更大范围内体现出共识机制的公平性和节点参与度.

以上分析表明需要设计一种新的共识机制或改进现有的 PoC 机制,在确保贡献值越大的节点具有越高的记账概率前提下,能够确保系统在任何情况下都有节点可以记账出块,作为灾备方案,解决

由于节点异常而无法正常记账出块的问题，提高共识机制的可靠性及可用性.因此，针对基于贡献值的区块链共识机制存在的缺陷以及区块链系统应用的实际需求，本文提出一种基于贡献值和难度值(PoC+PoW)的高可靠性区块链共识机制，根据贡献值排序为区块链网络中的节点分配 PoW 的难度值，节点再通过参与 PoW 竞争，最终确定区块链系统节点的记账权，确保记账出块率达到或无限趋近100%，维持区块链系统的正常运行.

本文首先介绍相关工作，重点是对“基于贡献值证明”共识机制的原理、核心理念、关键算法流程、安全性以及其存在的缺陷等方面进行介绍，奠定本文研究中所提共识机制的背景与基础.随后，本文对改进的区块链共识方案的核心设计思想以及所采取的关键技术进行详细的介绍，重点阐述“引入 PoW 竞争”、“基于贡献值分组”、“难度分配算法”三方面的技术及在所提共识机制中的必要性和可行性，并对节点获得共识的过程进行阐述.本文还针对所提的共识机制进行了两部分实验，第一部分是从多方面多变量验证算法设计的合理性，第二部分是与 PoC 进行对比性实验，验证改进后的共识机制的优越性与可靠性.

本文一共分为 6 节.

第 1 节 引言对所研究的问题、研究该问题的背景与意义、面临的挑战和针对这些挑战提出的解决思路进行说明；

第 2 节 相关工作对所研究问题的知识基础和近期的国内外相关研究进行阐述与说明；

第 3 节 PoC+PoW 核心设计思想对所提共识机制的核心设计思想和流程进行介绍；

第 4 节 PoC+PoW 技术设计与实现介绍 PoW 竞争、分组算法、难度分配算法以及共识数据计算四个方面的内容；

第 5 节 实验与分析从两个方面进行了实验.第一部分实验的目的是验证本文方案中提出的难度值分配方式和分组方式的合理性与可行性；第二部分实验的目的是验证本文所提共识方案的可行性，将共识方案部署在实际的局域网区块链系统中进行实验，并与传统的 PoC 方案进行对比，验证 PoC+PoW 方案所具有的优势；

第 6 节为结论与展望，对全文进行总结，并对本文所提共识做出更多的思考与展望.

2 相关工作

2.1 基于贡献值证明的共识机制

贡献值证明机制(Proof of Contribution，PoC)将节点对系统所的做贡献值(Contribution Value)作为决定节点记账权的关键指标，是一个根据节点贡献大小决定节点获得当前轮记账权的机制.PoC 共识机制根据贡献值算法，将用户对知识产权创作、交易等行为以贡献值的形式进行量化，其设计思路也适用于可以对用户在系统的行为进行量化的其它区块链应用系统.该共识机制规定由贡献值最大的节点获得新区块的记账权，体现出“按劳分配、多劳多得”的价值理念，激发节点参与区块链维护的积极性，提高区块链系统的安全性.

在基于 PoC 的区块链应用中，每个节点都参与维护一个相同的区块链账本，账本中的数据是系统中多项可自行计算数据的主要来源.账本中除了记录节点的各类行为数据，作为计算节点贡献值的基础，还记录着系统内节点的列表及其它相关信息.

PoC 的设计要求维护一个系统在线节点列表.一个节点 m 判断另外一个节点 w 的有效初入系统时间(Effective start time，Est)的过程如下：节点 m 在收到节点 w 发送的区块 b 时，首先对块 b 的地址信息与区块链账本中的节点列表信息进行比对，若判断该地址为节点列表中不存在的节点，则认定节点 w 为一个新加入节点.此时，区块 b 所包含的时间戳信息将作为节点 w 的有效初入系统时间.节点 m 将更新本地区块链账本中节点列表，将节点 w 的地址以及有效初入系统时间 Est 记录在其所维护区块链账本中的节点列表中.

节点贡献值计算的数据来源主要为节点的区块链账本，但也可以包含多个方面的数据.在本文的 PoC 中，节点的贡献值主要基于三个方面的数据统计：知识产权数据、知识产权交易数据以及节点在线时长数据.贡献值的计算可以根据不同的区块链业务场景和需要来丰富数据或增加其它系统设置数据，如在线时长可以选择持续在线时长或累计在线时长.设计的贡献值算法得到全网共识，节点可通过读取区块链账本中数据和其它系统数据来独立计算并得到各个节点当前的贡献值.

2.2 PoC 共识机制核心步骤

PoC 共识机制的简要流程分为以下 3 个步骤：

(1)假设参与贡献值积累周期 T 的节点数为 N,各节点通过获取系统中的知识产权注册数据和交易数据等行为数据来计算各节点的贡献值;

(2)在周期 T 结束时,节点经过本轮贡献值积累后拥有相应的贡献值,贡献值最高的节点(N_{hc})成为本轮的记账节点.在 N_{hc} 记账出块过程中,其它节点处于等待状态,无需其它实际动作;

(3) N_{hc} 完成记账出块后,系统将其贡献值归零,所有节点进入下一轮的贡献值积累窗口,参与下一轮的记账权竞争,即重复以上两个步骤.

2.3　PoC 共识机制存在的缺陷

由于与贡献值高低存在紧密耦合的关系,PoC 共识机制中的记账权本身具有了"确定性"(Deterministic)的特性.通过大量针对 PoC 共识机制的实验发现,"确定性"这一特性的副作用以一定的概率在移动网络环境不稳定、节点动态性高的公有链中复现,一旦获得本轮记账权的节点在记账出块过程中发生非正常下线、宕机而无法正常完成记账出块或者区块信息无法有效同步的情况,系统内其余节点均无力感知,只能处于被动等待状态,将导致系统运行的长时间挂起.因此,有必要为 PoC 共识机制中的节点记账出块设计灾备方案,此方面的研究存在很大的改进与扩展空间.

3　PoC+PoW 核心设计思想

本文提出一种结合贡献值和难度值(PoC+PoW)的区块链共识机制,引入 PoW 作为 PoC 共识机制的节点记账出块灾备方案,旨在消除 PoC 确定节点记账权中"确定性"(Deterministic)特性带来的可靠性问题.PoW 的引入能够进一步完善 PoC 共识机制中节点记账权竞争机制,在尊重 PoC 中"贡献值=记账权"强关联的同时,降低系统在运行过程中无法正常记账出块的概率,提高区块链系统的可靠性、健壮性与可用性.

PoC+PoW 共识机制的主要设计思想如下:首先,要确保贡献值排名最高的节点具有最高的记账出块概率;其次,随着节点贡献值排名的下降,节点记账出块概率要按照某种规律递减.本文的重点是设计出一个合理的 PoC 贡献值与 PoW 难度值之间的映射关系,即以 PoC 贡献值排名作为映射函数的输入变量,映射函数的输出结果既是 PoW 难度值,由此在节点贡献值排名与所分配的哈希值计算难度值之间建立起一个映射关系.基于贡献值和难度值的区块链共识机制流程如图 1 所示.

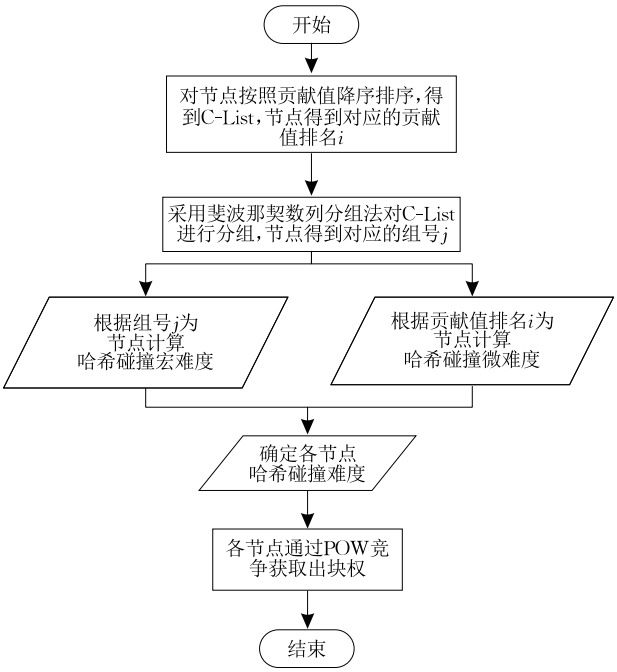

图 1　基于 PoC+PoW 的区块链共识机制流程

以下对 PoC 贡献值到 PoW 难度值的映射函数设计思路进行简要介绍.在经过 PoC 共识之后,各个节点已经获得了通过积累所形成的新的贡献值.此时,系统根据贡献值对节点从高到低进行一个排序,再运用斐波那契数列对排序后的节点进行分组,具体的分组方式是将斐波那契数组中第 n 个数值的大小设置为区块链系统中第 n 个组的节点数.完成分组后,组间节点将会分配到有不同个数前置零的哈希计算难度值,称为"宏难度",使组与组的节点之间的难度值具有本质差别;组内节点则根据贡献值排名,进行难度值微调,称为"微难度",使组内节点的难度值之间存在细微差别.执行上述分组和难度值方案后就确定了区块链各个节点的 PoW 难度值.然后,节点根据各自的 PoW 难度值进行挖矿竞争,确定此轮的记账与构建区块权.

4　PoC+PoW 技术设计与实现

4.1　引入 PoW 竞争机制

传统 PoW 共识机制的本质是确定工作量证明的难度值.与 PoC 相结合,则根据贡献值排序,系统给每个节点分配不同的难度值,然后节点使用 PoW 竞争机制,通过完成工作量而获得记账权.在当前轮区块构建完成之前,所有节点均参与竞争记账权,都

有机会获得构建新区块的权利，因此系统不会出现运行停滞的情况. 而 PoW 难度值的衡量标准是哈希计算难度值中前置零的个数，前置零个数越多，节点通过寻找符合难度值要求的正确答案概率越低，即难度越高.

通过引入 PoW 进行竞争记账权，在原有 PoC 机制中的一轮贡献值积累结束时，根据此时的贡献值给每个节点分配与贡献值成反比例的难度值，此后所有节点遵循 PoW 规则竞争记账权. 此方案在充分尊重 PoC 中“贡献值排名越靠前，获得记账权的概率越高”设计前提下，打破 PoC 共识机制的“确定性”(Deterministic)造成的节点“不作为”窘境，为确定性记账权增加非确定性(Non-deterministic)因素，贡献值排名靠前的节点拥有更高的获取记账权概率，贡献值最大的节点自然就拥有最高的概率获取记账权，但是在记账出块完成之前，其它节点也有竞争记账权的机会.

将 PoW 引入 PoC 也形成对 PoC 的一种灾备方案，如果本轮贡献值最大节点由于不明原因无法正常记账出块，则本轮贡献值排名第二的节点将有更大机会竞争获得记账权，以此类推. 因此，将 PoW 竞争机制引入到 PoC 机制可以有效避免由于记账节点宕机而造成系统运行出现停顿的情况发生. 此外，根据 PoW 竞争规则，贡献值不高的节点也有一定的概率(虽然较低)获得记账权，从而可以在一定程度上提高区块链中节点参与的积极性.

4.2 基于贡献值的分组算法

4.2.1 难度定义

PoC+PoW 共识机制兼具“贡献值”和“难度值”两个记账权量化因素. 在本方案的设计中，节点参与竞争的哈希计算难度分为“宏难度”和“微难度”两个层次.

定义 1. “宏难度”描述分组后组内节点所拥有相同层次的难度值，用于在组与组的节点之间形成难度阶梯，以传统 PoW 共识机制难度值中前置零的个数决定难度，根据分组算法产生的组号决定.

定义 2. “微难度”描述分组后在“宏难度”基础上对处于统一组的内节点赋予的难度增量，用于对组内节点的难度值进行微调，体现组内节点的贡献值排序.

本方案采用的分组策略使组与组之间节点的“宏难度”由难度值的前置零个数决定，形成难度梯队，同时组内节点根据贡献值排名进行微调，为节点增加一个基于贡献值排名的“微难度”.

4.2.2 分组策略及必要性分析

在每一轮 PoC 取得共识后，每个节点都有一个贡献值. 本方案将节点按照贡献值由大到小排序得到 C-List. 如果仅根据节点的排名 i 直接给节点分配难度值，则当 C-List 中排名靠前的节点之间的贡献值相差细微时，记账概率将几乎均匀分布在这几个节点之间，将违背 PoC 共识机制的本质，无法完全体现“尊重贡献值排名”的初衷. 因此引入一个分组策略，通过设置不同组之间节点的难度差值，确保加入 PoW 改进后的 PoC 共识机制仍然秉持基于贡献值的核心思想完成共识.

本方案拟采用基于“斐波那契数列”的分组策略. 经过深入分析与验证，该分组方案具有较高的效率，同时可以按照贡献值排名对节点设计合理的难度梯度，保证节点记账权以贡献值为主要决定因素，确保节点竞争的公平性和积极性. 以下将从分组效率和遵循 PoC 原则两个方面分析该分组方案的必要性.

定义 3. 设 $F(n)$为该斐波那契数列的第 n 项($n\geq 3, n\in N^*$)，满足以下条件的线性递推数列称为斐波那契数列：

(1) $F(1)=F(2)=1$；

(2) $F(n)=F(n-1)+F(n-2)$.

基于斐波那契数列特性的分组使按照 F 数列实现的分组将呈现以下特性：随着分组数量的增加，即随着组号的增大，组内成员的数量呈现阶梯式递增. 因此，本文方案的节点分组算法随着系统节点数的增加，会将大量处于较低贡献值范围、贡献值排名较后的节点划分在同一组内并赋值同样的“宏难度”，具有较高的分组效率. 分组方案表明，组内节点越多，在贡献值链上所处的位置就越低，而节点之间竞争成功的概率就越高，但是对于颠覆基于贡献值确定记账权原则的概率也就越低.

通过以上分析可以看到，本文提出的共识方案虽然增加了 PoW 机制对记账出块提供可靠性保障，但从本质上仍然维持 PoC 机制的“贡献值排名=记账出块权”高耦合关系.

以下通过三种场景分析“斐波那契数列分组法”的适用性与优势. 经过分组后，各节点的 PoW 难度值应该符合以下的假设情况：

(1) 贡献值排名第一的节点独立成为一组，难度值设定上拥有最少个数的前置零，即排名第一的节点相对其它节点来说具有最低的“宏难度”；

(2) 同组内节点的 PoW 难度值根据贡献值排

名进行微调而确定,在“宏难度”基础上增加相对应的“微难度”;

(3)同组内的节点即使出现贡献值相差较大的情况,也不会对系统的整体公平性产生根本性影响.

在场景(1)下,贡献值排名第一的节点对应的难度值,会与排名第二的节点对应的难度值之间存在一个急剧的落差,从而确保即使第一名与第二名的贡献值很接近,通过将它们划分到不同的组中,再对组设置不同的前置零个数控制其难度值差,能够确保拥有最高贡献值的节点独立成组,在难度设定上拥有的前置零个数最少的优势,在具体实现中通常设置一个难度与其它节点相比较低的值,以确保在此节点正常运行情况下最大概率地获得记账权.

在场景(2)下,随着节点数量规模的增大,可能出现竞争力的分水岭.采用斐波那契数列分组的结果是,对于贡献值排名越靠前部的节点,贡献值重要性越高,而组内节点个数越少,通过竞争获得记账权的概率越大,因此在最大程度上能够尊重 PoC 贡献值进行记账;对于排名越靠后部的节点,贡献值重要性越低,而组内节点个数越多,虽然依然尊重 PoC 贡献值排名,但通过 PoW 竞争获得记账权的概率越低,排名相近的节点根据“微难度”设置的难度值竞争记账权,在一定程度上可以激励系统节点的参与积极性和活跃度.

在场景(3)下,“斐波那契数列”分组法之后同组内存在的节点将具有相同的“宏难度”,即时两者之间具有较大的贡献值差别,通过“微难度”调整,组内节点也会有不同的竞争记账概率,且对于本身的贡献值排名并不靠前的节点其本轮出块优势本身也并不高,在确保系统可靠性的同时,不会对系统的整体公平性产生颠覆性影响.

如果使用普通的诸如均匀分段赋值“宏难度”的分组方法,首先系统节点数量越多,分组和赋值的操作重复次数越多,是一种较为低效的分组策略.其次将贡献值排名靠前的节点分配到同一组中,无法从本质上区分出 PoW 竞争难度,会大幅提高违背遵循 PoC 共识机制原则的可能性.

综上分析,本方案采取“斐波那契数列”分组法在分组效率和秉持遵循 PoC 原则确定记账权两个方面均具有明显优势.在效率方面,对于处于贡献值链上低值范围、记账权竞争优势不大的节点来说,可以通过斐波那契分组算法直接进入同一组中以获得相同的“宏难度”,降低多段难度赋值算法的复杂性,有效提高分组效率;在遵循 PoC 原则确定记账权方面,分组后的节点通过 PoW 竞争仍然能够确保共识机制最大程度上尊重 PoC 共识机制的贡献值排名,组与组之间形成“难度梯度”,保障记账权与贡献值的紧密相关性.同时,贡献值排名相近的各节点也能通过合理的竞争更加积极活跃地参与记账权的竞争,而同组内节点即使贡献值差值较大也不会对系统整体的公平性产生颠覆性影响.

4.3　难度值分配算法

4.3.1　算法描述

基于 PoC+PoW 的高可靠性区块链共识机制中的贡献值-难度值映射算法如算法 1 所示:

算法 1.　难度分配算法.

输入:i(节点的贡献值排名),n(系统节点总个数)

输出:H_i(节点的 PoW 难度值)

过程:$Function\ Difficulty(i,n)$

```
IF i=1 THEN
    param2=0;
ELSE
    param2=pow(c(i)−c(i−1),1/a);
Hi=pow(2,256−Dap−param1−param2)
RETURN Hi
```

以上难度值分配算法中的各项表达式定义如下:

$H_i=2^{256-Dap-param1-param2}$,

$$param1=j*\left\{\frac{\left(1+\frac{\lambda}{n}\right)\left(n+\frac{\lambda}{\sigma}\right)}{n+1}\right\}^{n+\frac{j}{n}},$$

$$param2=\begin{cases}0, & i=1\\ (C_i-C_{i-1})^{\frac{1}{\delta}}, & i>1\end{cases},$$

$\lambda=1+\dfrac{i+j}{n}(1<\lambda<3)$.

其中:

(1)i 表示节点的贡献值排名;n 代表系统节点数;j 表示排序为 i 的节点采用“斐波那契数列”分组法后获得的组号;

(2)H_i 表示贡献值排名为 i 的节点的 PoW 难度值,在随后的 PoW 竞争中,节点需要找到一个小于或等于 H_i 的哈希值,从而获得记账权;

(3)$\lambda=1+(i+j)/n(1<\lambda<3)$ 是系统难度控制因子;

(4)C_i-C_{i-1} 是第 $i(i>1)$ 个节点的贡献值与前一个节点的贡献值之差;

(5)σ 和 δ 是两个调节因子,其中 σ 在取 3 时可以使贡献值排名第一的节点的记账出块率符合最优预期,δ 是基于(C_i-C_{i-1})所处数值范围的一个动态调整的因子,不同的应用系统可以根据系统自身相关值的预设(比如贡献值分布范围)来确定该值的大小,即实现系统贡献值的归一化操作.

(6)Dap(Difficulty Adjustment Parameter)是难度值调节参数,用于调节系统整体的难度水平,控制记账出块的速度.通过对后文描述的实验结果进行分析,Dap 设为 16 则难度适中,可以较快地出块,同时降低分叉概率,降低因触发分叉处理程序而引起的额外时延.

4.3.2 算法设计几点说明

(1)随着节点贡献值排名 i 的增大,H_i 的数值会变小,节点 i 在进行 PoW 竞争时找到满足哈希值小于 H_i 的概率将会变小,即 PoW 的竞争难度变大;

(2)节点的 i 值越大,其经过"斐波那契数组"计算后所划分归属的组号 j 也就越大,H_i 会随之有小幅度的变小,即节点所处组的组号越大,PoW 难度也就越大;

(3)C_i-C_{i-1} 是排名为 i 的节点与排名为 $i-1$ 节点的贡献值之差,该值越大,H_i 就会越小,即 PoW 的难度会越大,符合"将节点间的贡献值之差作为决定难度的主要因素"这一设计思路.

4.4 基于账本数据的计算

4.4.1 数据计算

前文描述中提到,在节点维护的区块链账本中,有一个系统有效节点列表,记录从系统运行开始至今有记账记录的有效节点.各节点可通过遍历自己维护的列表,自行计算自己的排名情况;然后调用节点分组算法,输入贡献值排名 i,获得所在组的组号 j;再通过难度值分配算法计算出难度值 H_i,各节点随即基于 PoW 工作量证明机制竞争记账权.因为难度分配算法和分组算法全网共识,以上数据节点可根据算法自行计算.

4.4.2 分叉问题的解决

传统 PoC 共识机制可以通过合理设计贡献值积累算法,丰富贡献值计算所使用的相关影响因子而做到贡献值相同的情况几乎不会发生,从而降低区块链分叉的可能,保证区块链系统的安全性和抗攻击性.然而,一旦出现分叉,本文提出以下解决策略:

(1)对于贡献值相同的节点,基于时间戳决定记账权.若存在多于一个节点具有相同的贡献值,根据 PoC 规则,这些节点将拥有相同的排名 i,根据难度分配算法,都将获得相同的 PoW 难度值.最终记账权则由最快完成记账出块的节点获得,即通过 PoW 决出工作量最大的节点,以区块构建时的时间戳为准.

(2)对于贡献值不同但由于使用 PoW 而同时获得记账权的节点,则以贡献值排名靠前的节点所构建的区块作为最终入链区块.

(3)在极端情况下,贡献值相同又同时在 PoW 竞争阶段构建的区块有相同的时间戳,则按照节点有效初入系统的时间(Effective start time,Est)为准,相对较早加入系统的节点所完成的区块为最终入链区块.

4.5 安全性分析

4.5.1 安全攻击分析

(1)共谋攻击

共谋攻击原指在区块链中,矿工可能会发起矿工共谋攻击,即大多数攻击,以实现利润最大化.在本文所提共识机制中可能出现的共谋攻击为节点合谋通过手段转让贡献值给某一节点,使其总是具有最高贡献值,从而具有更大的成块几率;或者相反,共谋不去通过某个节点的出块,使其无法合理地获取到应有的贡献值.这样的攻击同样地打击了系统内诚实节点的积极性.

(2)Spam 攻击

Spam 搜索引擎垃圾技术,最初是专门指欺骗搜索引擎的行为,不诚实的网站管理员利用不道德的技巧欺骗搜索引擎,从而在短时间内获得排名的提高.这种不诚实节点为了恶意骗取贡献值,短时间内向区块链系统频繁上传低质量信息,从而造成 Spam 攻击.实际上,Spam 攻击从本质上来说与共谋攻击想要达成的目的是一致的.

综上对两种安全攻击的分析,在 PoC+PoW 共识机制中,需要有相应策略来对以恶意提高本身贡献值为目的的节点进行防备.

4.5.2 PoC+PoW 的安全策略

(1)海绵函数

PoC 共识机制作为一种将贡献值作为主要因素来决定节点记账权的共识算法,从安全性角度对贡献值算法进行了优化.为了防止攻击者短时间内向系统大量上传无意义作品骗取贡献值,以及因共谋导致的某节点在短时间内多次确权的行为,PoC+PoW 共识机制设定了一个"海绵函数"算法流程描述见算法 2.

算法 2.　海绵函数.

输入:T(收益冷却周期),t(相邻确权行为间隔时间),n(用户进行确权的作品数量),$upperLim$(单次知识产权确权能获得的贡献值上限)

输出:Dpc(节点当前知识产权确权行为所得贡献值)

过程:$Function\ Sponge(T,t,n,upperLim)$

IF $t>T$ THEN

$Dpc=upperLim$;

ELSE

$Dpc=F(T,t,n,upperLim)$;

RETURN Dpc

众所周知,知识产权的前期创作和确权操作需要通过一定时间积累,一般情况下用户知识产权确权行为不应在短时间内频繁发生.结合知识产权这一产品的特性,海绵函数在贡献值算法中加入了时间纬度.若在短时间(或系统预设时间长度)内出现多次的知识产权确权行为都来自同一用户,则该用户获得的贡献值收益值会瞬间降低,只有经过时间推移,确权带来的贡献值收益才会逐步回升至正常水平.对于确实在短时间内有对大量知识产权进行确权需求的用户(如企业用户),贡献值收益水平的降低和逐步回升并不会影响用户正常使用区块链提供的确权与交易服务.

如图 2 所示,假设将贡献值收益冷却周期 T 设为 10 min(600 s),单次知识产权确权行为所得贡献值的上限值($upperLim$)设置为 5,则某用户在 300 s 时进行了知识产权确权,获得的贡献值为 5;10 min 后,即 900 s 的时刻用户又进行了知识产权确权,获得的贡献值仍为 5.但在第 1200 s 用户再次发生知识产权确权行为,由于其尚未度过收益冷却周期,用户获得的贡献值奖励仅为 1.25 并且重新进入新的冷却周期.在经过完整 10 min 的冷却期后,在第 1800 s 时再进行知识产权确权所获得的贡献值才恢复为 5.

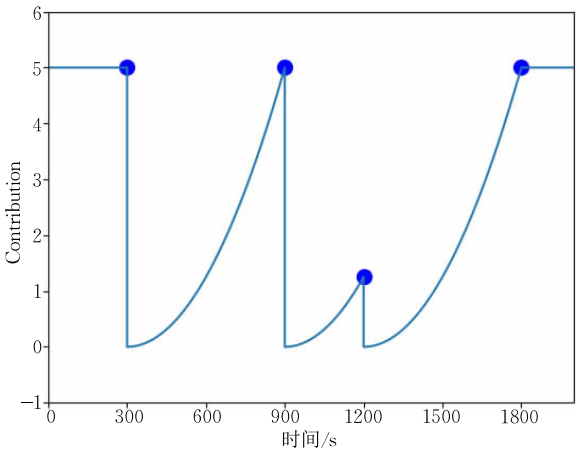

图 2　PoC+PoW 海绵函数贡献值增长曲线

通过"海绵函数"机制的设计,PoC 能够对恶意提高本身贡献值的节点进行合理干预,既可以防止不诚实节点形成 Spam 攻击,也不会影响诚实用户正常使用系统业务并获得贡献值带来的相应奖励.PoC+PoW 中这一机制的设计可以提高节点参与区块链网络的积极性,扩大网络规模,有利于保障区块链的安全性.

(2)贡献值使用即清零机制

传统 PoC 中规定在出块节点成功出块后,其贡献值会被归零,需要较长一段时间贡献值积累才能恢复到竞争较高概率出块权的水平,以达到维护节点出块权竞争公平性的目的.如果出现合谋攻击,节点使用某种手段将自己获得贡献值的机会让给同一个节点,即使该节点完成出块,并获取了收益.但是无论是对于受益节点,还是转让贡献值的节点,他们的所获收益均不高,没有支撑他们进行合谋攻击的动力.

(3)灵活的奖惩机制

PoC+PoW 鼓励使用本共识机制的系统制定灵活的奖惩机制,对于成功出块节点给予奖励,同时制定平衡机制,可通过调节获得贡献值的收益和确权或交易需要付出手续费之间的关系来提高攻击者的攻击成本.也可以通过对恶意行为的检测手段按比例降低该行为的收益值.

5　实验及分析

本文将从两个方面进行实验.第一部分实验的目的是验证本文方案提出的难度值的合理性与可行性,将通过设置不同变量、从多个角度验证共识机制的合理性.第二部分实验的目的是验证本文所提共识方案的可行性,将共识方案部署在实际的局域网区块链系统中进行实验,分别从节点实际记账情况 PoC+PoW 和预定记账节点出现异常下线情况时的灾备能力进行实验,并与传统 PoC 方案进行对比,验证方案具有的优势.

5.1　PoW 共识机制难度值合理性验证

根据本文设计的难度计算公式为各节点分配 PoW 难度值,实验模拟面向知识产权保护与交易的区块链系统中节点进行每一轮竞争记账权及完成新区块的创建.该实验围绕本文设计的 PoC+PoW 共识方案,从系统节点数、相邻节点间贡献值之差、分组方式多个维度进行实验,验证难度值分配方案设

计的合理性.

5.1.1 实验设置

(1)数据预处理.针对不同的实验自变量与因变量,设计制定量化的贡献值降序列表.列表中的数值根据贡献值列表生成算法基于系统节点总数 N、节点间贡献值差值 gap 等预设测试值计算得出.选取列表中排名前 1/3 的节点赋予大于 0 且依次以差值为 gap 递减的贡献值,其余节点的贡献值均初始化为 0.此设置根据本方案"获得记账权的概率随着贡献值的降低而降低"规则,记账节点将从排名前 1/3,甚至更小范围内产生.在理想的情况下,贡献值排名第一节点获得记账权的概率应达到或无限接近 100%.

(2)实验数据产生.每组实验完成 50 次通过 PoW 竞争取得记账权,记录各个节点的记账次数,实验重复 10 次.最终统计出 PoC 贡献值排名前十的节点在 50×10=500 次 PoW 竞争中各自获得记账权并完成构建区块的概率.

(3)实验平台配置.本实验通过多线程编程模拟节点,使用的系统为 MacOS Mojava 10.14.6,处理器为 2.7 GHz Intel Core i5,内存为 8 GB,使用 Golang 语言编程实现.

5.1.2 系统节点数 N 对节点记账出块概率的影响

实验分别将 N 设置为 100、200、300、400 和 500,目的是分析系统节点数 N 对于节点通过 PoW 竞争取得记账权概率的影响.同时另外增加两组对比实验,将 N 设置为 5000 和 50000,与 N 为 500 形成数量级增长的情况进行对比分析.

图 3 中的实验结果表明,对于不同系统节点数 N,系统中前十节点获得记账权概率曲线的趋势基本保持不变.从而可以得出以下结论:区块链系统规模对于贡献值排名第一的节点来说,通过 PoW 竞争机制获得记账权的概率可以得到充分保障,与此

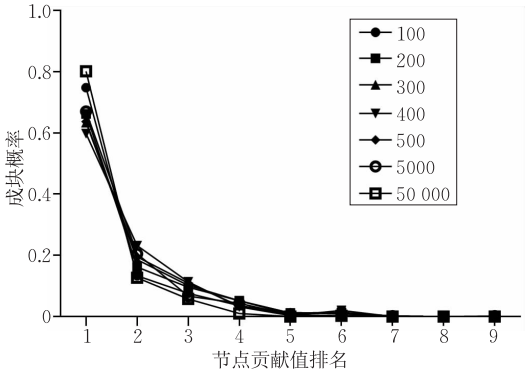

图 3 系统节点数与节点获得记账权概率的关系

同时,系统中其它节点获得记账权的概率变化曲线趋势也没有随着节点个数 N 值的变化而产生明显不同.因此,本文设计的 PoC+PoW 共识机制对于系统规模来说具有良好的适应性和鲁棒性.

5.1.3 节点贡献值差对节点记账概率的影响

为了确保系统共识机制的公平性,防止出现某些节点在贡献值差别很小的情况下,由于贡献值排名的不同,而出现 PoW 难度值差别很大的情况.本文设计的共识机制将节点间的贡献值之差也作为一个难度控制因子,用 PoC 贡献值排名序列中一个节点与前一个节点间贡献值的差值代表,该差值越大,则 PoW 难度值的差值就会越大,排名靠后节点通过 PoW 竞争取得记账权的概率就越低.

为了分析节点间贡献值差异对于节点取得记账权的概率的影响,设计了如下实验:设置贡献值排名第一的节点和排名第二的节点的贡献值差值 gap 分别为 5,10,15,20,25,并设置其它节点之间贡献值差值均为 5,分析节点间的难度差异对节点取得记账权概率的影响.图 4 是在不同 gap 情况下,节点通过 PoW 竞争获得记账权概率曲线.实验结果表明,根据排名为第一和第二两个节点获得记账权概率曲线的斜率可以看出,获得记账权概率之差随着贡献值之差的增加而增加,设计符合"将节点间的贡献值差值作为难度值的影响因素"的设计思路.

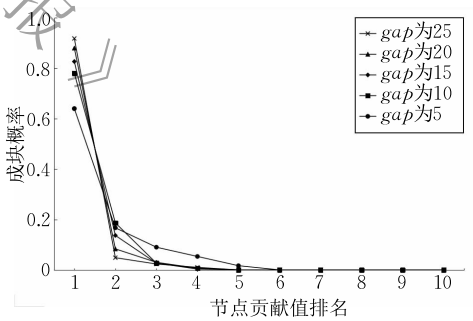

图 4 贡献值之差与节点获得记账权概率的关系

5.1.4 斐波那契数列分组方案合理性

为了确保区块链系统共识机制的公平性和合理性,本方案基于"组间节点难度通过前置零个数控制,而组内节点难度通过贡献值排名控制"的设计思路,对各节点合理分配难度值,保障节点获得记账权概率的合理分布.

本方案采用斐波那契数列对贡献值有序列表 C-List 进行分组,组号 j 作为难度分配的一个影响因子,排名靠前的节点将获得大的难度分配优势.

为了检验分组方式对节点获得记账权概率的影

响,设计了以下实验:针对难度值分配,分别采用斐波那契数列分组法和平均分组法,为节点计算出对应分组的组号 j;在平均分组方案中,将 C-List 按照每 3 个节点归为一组的方式.在以上两种组号获取算法中,输入均为节点的贡献值排名 i,输出为节点所在分组的组号 j.组号确定后,再进行难度计算,得出节点的 PoW 难度值.

在对两种分组方式分别进行实验中,设置系统节点数为 500、节点间贡献值差值均为 5,实验重复 500 次,得到贡献值排在前十名的节点通过 PoW 竞争获得记账权的概率曲线,如图 5 所示.实验结果表明,使用平均分组法,得到的曲线起伏较大,相邻节点之间的获得记账权概率更加趋于接近,没有与贡献值维持明显的正相关的关系,在统计实验结果中也出现记账出块节点是前十名之外节点的情况,即前十名节点的记账出块率无法达到 100%.而使用斐波那契数列分组法得到的概率曲线是规律、平滑的反函数曲线,同时,根据实验统计结果,记账出块节点均为排在前十名的节点,即前十名节点的记账出块率达到 100%,符合本方案设计思想,即尊重贡献值的区块链共识机制.

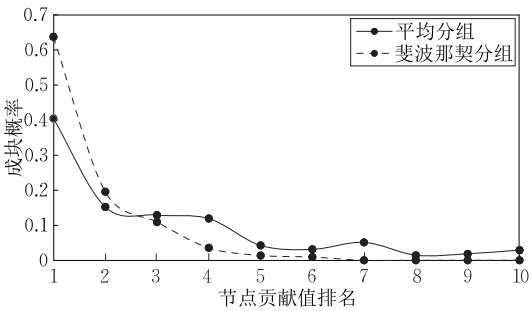

图 5　分组方式与取得记账权概率的关系

5.2　与传统 PoC 共识机制对比实验

在基于 PoC 共识机制的区块链系统中,设置了一个出块阈值 T,代表当前一轮的业务量.当区块链系统中交易的业务量达到出块阈值 T 时,PoC 根据节点在上个共识周期结束时的贡献值情况,由具有最大贡献值的节点创建新区块.为了与 PoC 共识机制进行对比,将从出块时间延时和灾备能力两方面进行实验设计以及结果分析.

5.2.1　实验设置

(1)实验思路

设定出块阈值 T 为交易量 5,当到达阈值 T 时,节点通过对各自维护的节点列表中信息进行计算可以得出自己的贡献值、贡献值排名等,在计算出 PoW 难度值并通过竞争获得记账权,最后由成功获得记账权的节点构建新区块.

(2)实验平台设置

本部分实验的环境为由局域网(不考虑网络时延)内的五台计算机模拟系统内节点,其中 4 台为台式机,1 台为笔记本,配置如表 1 所示.

表 1　实验用计算机配置情况

CPU 型号	CPU 主频/GHz	内存/GB	操作系统
Intel Core 2	2.6	4	Windows 10
Intel Core i5	2.7	8	MacOS Mojava 10.14.6

5.2.2　记账出块时延实验

本实验用于对记账出块耗时进行统计分析,分别针对难度公式中难度调节参数 Dap 选取 14～19 之间的值进行实验.对于每一个实验设置,分别统计记账构建 100 个区块所需的平均出块时延.

图 6 中的实验结果显示,在竞争记账权中基于 PoW 进行共识,出块时延会随着难度值的增加而增加.当难度值调节参数 Dap 设为 16 时,平均出块时延为 539.37 ms,对系统整体记账出块效率所产生影响可忽略不计.在实际应用中,可以根据运行环境及系统性能等条件对 Dap 进行调节,以满足系统对记账出块时延的要求.

5.2.3　灾备能力实验

本实验通过在 PoW 竞争记账权开始时,将贡献值最高的节点人为下线,以获得“贡献值最高节点异常下线”情况下的记账出块时延.在本实验中,如将难度调节参数 Dap 设置为 16 可以获得最短的灾备出块时延.

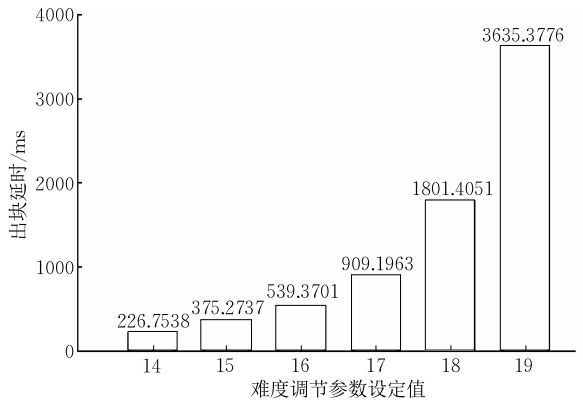

图 6　不同难度调节参数的平均出块时延

对实验结果进行统计,从贡献值最高的节点异常下线无法参与 PoW 竞争记账权,直到当前轮次正常出块的平均时延为 2.57 s.因此 PoC+PoW 作为 PoC 的一种灾备方案能够在异常发生时仍然能

够成功出块，并且对记账出块的时延影响不大.

在对选择不同 Dap 值时贡献值最高节点异常下线的场景进行实验后发现，在 Dap 值超过 16 时，由于其它节点的 PoW 难度设置较高，成功记账出块耗时较长.

图 7 展示贡献值排名前三的节点通过 PoW 竞争获得记账权构建区块的概率. 结果显示，在不同的难度调节参数 Dap 下，记账出块率均达到 100%，可以确保系统的新区块出块率，且每轮竞争获得记账权的节点均为贡献值排名前三的节点，充分体现了 PoC＋PoW 共识机制对贡献值的充分尊重，同时系统高出块率证明了该共识机制的高可靠性、灾备能力强.

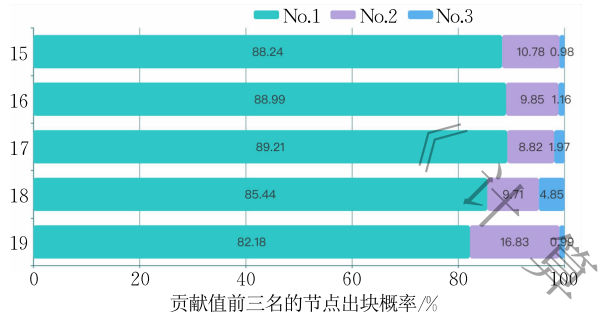

图 7 贡献值排前三名节点的出块概率

6 结论与展望

本文提出了一种结合贡献值和难度值的区块链共识机制，是一种根据节点贡献值来分配节点在 PoW 竞争中对应的难度值的共识机制，是对单纯的基于 PoC 共识机制的记账出块灾备方案，以改进系统运行的可靠性.

本文提出的 PoC＋PoW 共识机制主要针对 PoC 中的记账节点确定算法进行改进，设计难度值分配算法，在加入 PoW 竞争的同时，确保节点记账权仍然依据贡献值原则，同时激发系统节点参与竞争的自发性和活跃度. 本方案根据节点的贡献值排名为节点分配相应的 PoC 难度值，保证记账概率与节点贡献值排名成正相关性且记账出块节点集中在排名靠前的节点中. 从系统节点总数、相邻节点间贡献值之差以及分组方式三个角度，对难度值分配算法进行了设计，并通过实验验证了算法的合理性、正确性与可行性；同时在实际运行环境中进行对比实验，验证了所提方案的记账出块效率及灾备能力. 结合 PoC＋PoW 的高可靠性共识机制不但能够保证节点获得记账权概率与节点贡献值排名成正相关性，还能够保障节点参与竞争的公平性，是一种有效的确保系统能够平稳运行的解决方案.

本文所提的区块链共识算法还有很多可以改进的空间. 根据当前研究进展，未来 PoC＋PoW 区块链共识算法的研究方向可以在以下两个方面展开更深入的研究：

(1) 探索更加优化的分组方案. 本文中采用的“斐波那契数列分组法”在一定程度上保证了对 PoC 共识机制的充分尊重，但是不一定能够依照贡献值排序形成最优的分组，对贡献值进行聚类分组也许对于依据“宏难度”和“微难度”的思路确定节点的 PoW 难度值来说会是一种更好的分组结果. 我们将针对此问题继续研究优化方案，研究结果会在未来发表的论文中进行报告.

(2) 设计更加全面的难度分配方式. 本文中采用的难度分配算法主要从节点贡献值排名、所在组以及相邻节点贡献值差三个变量入手设计. 未来研究可以随着对“知识产权保护与交易”的应用场景以及将“贡献值”作为激励方式的区块链类应用探索的进一步深入对难度分配算法加入更多的影响因子，进一步提高算法设计的健壮性，优化算法运行的性能，使其适应于更多的实际应用场景.

参 考 文 献

[1] Pilkington M. Blockchain technology: Principles and applications //Olleros F X, Zhegu M, eds. Research Handbook on Digital Transformations. Edward Elgar, 2016

[2] Pierro M D. What is the blockchain? Computing in Science & Engineering, 2017, 19(5): 92-95

[3] Aras S T, Kulkarni V. Blockchain and its applications — A detailed survey. International Journal of Computer Applications, 2017, 180(3): 29-35

[4] Yuan Yong, Wang Fei-Yue. Blockchain: The state of the art and future trends. Acta Automatica Sinica, 2016, 42(4): 481-494(in Chinese)
(袁勇，王飞跃. 区块链技术发展现状与展望. 自动化学报，2016, 42(4): 481-494)

[5] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. White Paper, 2008

[6] Gribble S D, Halevy A Y, Ives Z G, et al. What can database do for peer-to-peer?//Proceedings of the 4th International Workshop on the Web and Databases. Santa Barbara, USA, 2001: 31-36

[7] He Pu, Yu Ge, Zhang Yan-Feng, et al. Survey on blockchain technology and its application prospect. Computer Science, 2017, 44(4): 1-7(in Chinese)

(何蒲，于戈，张岩峰等. 区块链技术与应用前瞻综述. 计算机科学，2017，44(4)：1-7)

[8] Han Xuan，Liu Ya-Min. Research on consensus mechanism in blockchain Technology. Netinfo Security，2017，(9)：147-152(in Chinese)
(韩璇，刘亚敏. 区块链技术中的共识机制研究. 信息网络安全，2017，(9)：147-152)

[9] Yang Yu-Guang，Zhang Shu-Xin. Review and research for consensus mechanism of block chain. Journal of Information Security Research，2018，4(4)：369-379(in Chinese)
(杨宇光，张树新. 区块链共识机制综述. 信息安全研究，2018，4(4)：369-379)

[10] Antonopoulos A M. Mastering Bitcoin：Unlocking Digital Crypto-Currencies. California，USA：O'Reilly Media，Inc，2014：173-214

[11] Olfati-Saber R，Murray R M. Consensus problems in networks of agents with switching topology and time-delays. IEEE Transactions on Automatic Control，2004，49(9)：1520-1533

[12] King S，Nadal S. PPCoin：Peer-to-peer crypto-currency with proof-of-stake. White Paper，2012

[13] Liu Yi-Zhong，Liu Jian-Wei，Yu Hui. Research on blockchain consensus：Comparison of typical schemes. ZTE Technology Journal，2018，24(6)：1-7(in Chinese)
(刘懿中，刘建伟，喻辉. 区块链共识机制研究：典型方案对比. 中兴通讯技术，2018，24(6)：1-7)

[14] Watanabe H，Fujimura S，Nakadaira A，et al. Blockchain contract：A complete consensus using blockchain//Proceedings of the 2015 IEEE 4th Global Conference on Consumer Electronics. Osaka，Japan，2015：577-578

[15] Kishigami J，Fujimura S，Watanabe H，et al. The blockchain-based digital content distribution system//Proceedings of the 2015 IEEE 5th International Conference on Big Data and Cloud Computing. Dalian，China，2015：187-190

[16] Liu W. Principles of blockchain technology and analysis of intellectual property services based on blockchain technology. Property Rights Guide，2016

[17] Tsai W，Feng L，Zhang H，et al. Intellectual-property blockchain-based protection model for microfilms//Proceedings of the 2017 IEEE Symposium on Service-Oriented System Engineering. San Francisco，USA，2017：174-178

[18] Ajay K，Bharath B，Akhil M V，Akanksh R，Hemavathi P. Intellectual property management using Blockchain//Proceedings of the 2018 3rd International Conference on Inventive Computation Technologies. Coimbatore，India，2018：428-430

[19] Zhu Lie-Huang，Gao Feng，Shen Meng，et al. A survey of blockchain privacy protection. Journal of Computer Research and Development，2017，54(10)：2170-2186(in Chinese)
(祝烈煌，高峰，沈蒙等. 区块链隐私保护研究综述. 计算机研究与发展，2017，54(10)：2170-2186)

[20] Shen Xin，Pei Qing-Qi，Liu Xue-Feng. Survey of block chain. Chinese Journal of Network and Information Security，2016，2(11)：11-20(in Chinese)
(沈鑫，裴庆祺，刘雪峰. 区块链技术综述. 网络与信息安全学报，2016，2(11)：11-20)

[21] Eyal I，Sirer E G. Majority is not enough：Bitcoin mining is vulnerable//Proceedings of the 18th International Conference on Financial Cryptography and Data Security. Christ Church，Barbados，2014：436-454

[22] He Jing-Sha，Wang Jian-Yu，Zhu Na-Fei，et al. Blockchain consensus method and device based on proof of contribution. Chinese Patent：CN109921909A，2019.6.21(in Chinese)
(何泾沙，王建宇，朱娜斐等. 基于贡献证明的区块链共识方法及装置. 中国专利：CN109921909A，2019.6.21)

HE Jing-Sha，Ph. D.，professor. His current research interests include network security，blockchain technology and digital forensics.

ZHANG Kun，M. S. candidate. Her research interests include blockchain technology and consensus mechanism.

XUE Rui-Xin，M. S. candidate. Her research interests include application of blockchain technology and the design of blockchain consensus mechanism.

ZHU Na-Fei，Ph. D.，associate professor. Her research interests include privacy protection，information security，blockchain technology.

HE Peng，Ph. D.，professor. His main research interests include transmission protocol and information security based on network time synchronization.

SONG Hong-Yu，M. S. candidate. His research interests include blockchain systems and consensus mechanism design.

DU Wei-Dong，M. S. candidate. His main research interests include blockchain technology.

GAN Yu，M. S. candidate. His major research interest is blockchain technology.

Background

The content of this paper belongs to the domain of the consensus mechanism of blockchain. Blockchain technology is characterized by decentralization，sequential data，collective maintenance，programmability，security and credibility. Data

in the blockchain is constantly updated in real-time according to the order of the time stamps, which can create an untamperable tracking record for the transfer of any asset without the need to seek the help of a trusted third-party. Consensus mechanism is the soul and law of blockchain, which maintains the normal operations of the blockchain system. In the blockchain, each node maintains the same ledger, and the allocation of accounting rights of the ledger is decentralized. When point-to-point transactions are very close in terms of time, sorting the transactions is decided by the consensus mechanism. Blockchain consensus mechanisms have been developed for over ten years and many types of mechanisms have been proposed as the result.

Most current Blockchain systems rely on the circulation of "coins" based on the proof of work (PoW) consensus mechanism. In view of the application scenarios of intellectual property protection and transaction, a consensus mechanism based the prove of contribution (PoC) has been proposed in which the contribution values of nodes are used as the key index to decide which node should get the right to construct the new block in each round. However, the PoC consensus mechanism exhibits the property of determinism, resulting in the possibility that if the selected node doesn't function correctly, system operation would hang and all other nodes would go into the waiting state. Apparently, there is the need to have a disaster recovery scheme for PoC to ensure continuous and smooth operation of Blockchain systems that employ the PoC consensus mechanism.

The Blockchain consensus mechanism proposed in this paper aims to improve the PoC mechanism by incorporating the PoW mechanism that would introduce non-determinism in the selection of the block-constructing node. From PoC to PoW, the difficulty values for PoW are determined by the ranking of the contribution values from PoC. This paper proposed an algorithm for the allocation of difficulty values to nodes based on the contribution values of the nodes to add some uncertainty while fully respecting the contribution values. The proposed scheme stimulates the spontaneity and activity of node competitions in the system. In the scheme, according to the contribution value ranking of the nodes, the corresponding difficulty values of competition in the PoW are determined for the nodes to ensure that the probability of constructing a block by a node is proportional to the ranking position of the contribution value of the node. The rationality, effectiveness and feasibility of the difficulty allocation algorithm is verified through experiment by examining three parameters: the total number of nodes in the system, the difference of the contribution values of adjacent nodes in the ranking, and the node grouping strategy. Experimental results also showed that the proposed scheme has improve the efficiency of block generation compared to PoC while possessing the capability of disaster recovery.

The proposed PoC + PoW consensus mechanism based on contribution values and difficulty values can not only guarantee the fairness of competition based on contribution values, but also ensure high efficiency of block generation. Experiments demonstrated that nodes that generate blocks are mostly distributed among the top ten nodes in the ranking list of the contribution values. The higher the ranking of a contribution value, the higher the probability of block generation by the corresponding node, and the probability of block generation by all the nodes can reach or approach infinitely to 100%, which can effectively prevent system hanging situations.