软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, [doi: 10.13328/j.cnki.jos.000000]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于组合特征双重加权的区块链共识机制研究*

金梦雪[1]，高鹏翔[1]

[1](青岛大学 数据科学与软件工程学院,山东 青岛 266000)

通讯作者：高鹏翔, E-mail: gaopengxiang@qdu.edu.cn

摘 要：区块链技术提供了全新的去中心化理念和分布式数据库底层框架逻辑结构.对区块链的核心技术共识机制进行了研究，从安全性、资源消耗、性能效率等方面对工作量证明机制（Proof Of Work, POW）、权益证明机制（Proof Of Rights, POS）等几种共识机制进行了对比分析.并提出了一种改良的共识机制--组合特征双重加权共识机制，按照组合特征加权的思想，筛选出最具代表性的节点，实现系统中各节点数据保持一致，保障了分布式系统的一致性和正确性，为区块链共识机制提供了基于 POW 和 POS 有机结合的发展方向.

关键词：区块链;共识机制;工作量证明机制;权益证明机制;组合特征加权

中图法分类号：TP309

Research on blockchain consensus algorithm based on combined feature double weighting

JIN Mengxue[1], GAO Pengxiang[1]

[1](School of Data Science and Software Engineering, Qingdao University, Shandong 266000, China)

Abstract: Blockchain technology provides a new decentralization concept and the underlying framework logic structure of distributed databases. Research on the core technology consensus mechanism of blockchains, From the aspects of security, resource consumption, performance and efficiency, several kinds of consensus mechanisms such as Proof Of Work (POW) and Proof Of Rights (POS) were compared and analyzed. And an improved consensus algorithm-Combined feature dual weighted consensus algorithm. According to the idea of weighting the combined features, the most representative nodes are selected to achieve consistent data of each node in the system, which ensures the consistency and correctness of the distributed system. It provides a development direction based on the organic combination of POW and POS for the blockchain consensus mechanism.

Key words: blockchain; consensus mechanism; POW; POS; Combined Feature Weighting

区块链本质上是一种去中心化的、可追溯的、对等的分布式数据库管理系统，在对等的分布式数据库管理系统中[1]，一切的节点共同参与保障分布式系统中各部分的有效运行，因此需要有一种准确高效的共识机制使分布式系统达成共识，图 1 为区块链去中心化网络拓扑结构示意图.共识机制是以分布式系统为基础的区块链技术的核心技术，本文着重研究了三种主流的共识机制基于节点算力的工作量证明算法（POW）[2]，基于货币拥有量的权益证明（POS）[3]，结合算力和货币拥有量的股份权益证明（DPOS）[4]的等基本共识机制思想.比特币作为区块链技术的典型应用，它采用基于随机散列[5]的工作量证明机制达成分布式系统各节点间共识.系统节点通过反复尝试寻找一个满足特定难度条件的哈希值随机数（SHA256 数学难题）[6]来完成一定的工作量证明，同时，该最先找到该随机数的节点获得本轮的记账权，验证通过将得到一定的比特币，最终工作量证明机制借助系统中节点间的算力竞争来保持分布式系统中各节点间数据的统一性和共识的快速安全性.权益证明机制本质上是拥有一定量货币的权益证明代替通过消耗不可再生资源产生哈希算力的工作量证明，POS 共识机制将投票权延伸至系统的利益相关者，依赖于股权证明[7]，参与者不会消耗稀缺资源，减少了资源的浪费.中本聪于 2010 年提出币龄概念[8]，即节点对特定数量货币的持有权，币龄是节点持有的货币量与该货币持有时间的乘积，POS 达成共识过程的难度系数与系统节点拥有的币龄成反比例，消费的币龄越

多则挖矿的难度值越低.

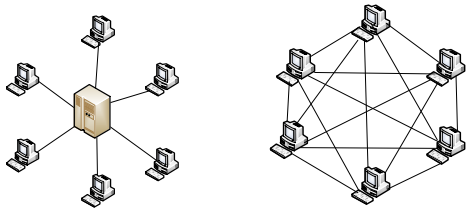

Fig.1 Centralization and blockchain decentralized network topology

图 1 中心化以及区块链去中心化网络拓扑结构

1 区块链的核心技术

2016 年，国家工信部在《中国区块链技术和应用发展白皮书》中对区块链技术进行了明确定义[9].相比于以往的中心化数据处理技术，区块链技术具备去中心化、安全可信、可追溯性、灵活可编程等优点.区块链技术采用密码学纯数学方法建立系统中各节点间的关系模型，图 2 为区块链的基础构架模型，增加了去中心化系统的可靠性，增加了系统的可信性；区块链技术采用具有单向特征和输出数值长度固定的哈希算法以及非对称加密算法[10]进行信息的加密，保证了数据的安全，并实现了借助工作量证明机制（POW）等共识机制使分布式系统中正常节点达成安全可靠、一致的网络状态的共识，依靠系统的强算力保证数据不可篡改、不可伪造，增加了信息的可靠性，具有较高的安全可信性；图 3 为区块链技术独有的区块加链式结构辅以时间戳功能，证明了数据的存在性增加了时间维度，增加了数据信息的可追溯性和可验证性；区块链技术的智能合约部分为系统提供灵活易于编程的脚本代码系统，区块链允许用户根据自己的需求制定和部署智能合约.例如，以太坊 (Ethereum) [11]作为区块链技术的另一成功应用，它提供了图灵完备的可准确定义的智能合约方便用户操作.

Fig.2 Blockchain infrastructure model

图 2 区块链基础构架模型

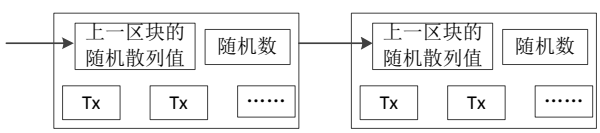

Fig.3 Chain structure of blockchain

图 3 区块链的链式结构

2 区块链与组合特征双重加权共识机制

本文提出一种新的基于组合特征双重加权共识机制，其基本思想为按一定的权重确定裁判节点，裁判节点按一定的权重投票选出代表节点，代表节点 90%达成一致意见通过验证，才能将新产生的区块加入区块链.图 4 为组合特征加权共识机制达成共识的流程图.

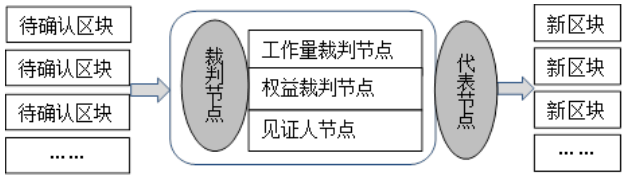

Fig.4 Blockchain feature weighted consensus mechanism

图 4 区块链的组合特征加权共识机制

组合特征双重加权共识机制达成共识的过程如下：裁判节点共 101 个，且裁判节点由“工作量节点”、“权益节点”、“见证人节点”等组成，分别代表区块链系统中不同性质的节点，工作量节点拥有很强的计算能力，权益节点主要依据拥有货币拥有量的多少选出，见证人节点要求节点在线的时间达到一定时限，其中，工作量节点 51 个，占总数的二分之一，权益节点 20 个，占总数的五分之一，见证人节点 30 个，占总数的十分之三.再由裁判节点选取代表节点，代表节点通过自我推荐或者从上一届裁判节点中选出，代表节点由裁判节点按一定权重通过投票产生，共选取代表节点 201 个.

Table 1 Distribution of two types of nodes: referee node and representative node

表 1 裁判节点、代表节点两类节点的分布

节点类型	工作量	储币量	在线时长	节点总数
裁判节点	51	20	30	101
代表节点	101	40	60	201

其中，每个节点提交一份该节点的工作日志档案，包括拥有的货币量、储币时长、一段时间总算力、节点当下的算力、未来预期的算力等，规定裁判节点必须在规定的时间内生成区块，否则，失去裁判权，重新选举出新的裁判节点.有恶意行为的、被记入黑名单的、离线超过一定时间的节点均无权参与裁判节点或者代表节点的竞选.

组合特征双重加权共识机制达成共识的过程包括三个阶段.

(1) 裁判节点的产生过程：将系统节点分别按工作量、储币量、在线时长排序；依次选出工作量前 51 名，储币量前 20 名，在线时长前 30 名节点，如有重复，依次顺延.除去不良节点，有恶意行为、被记入黑名单、离线时间超过一定时间的节点.依次选出 101 个节点，作为裁判节点.

(2) 代表节点的产生过程：代表节点的产生，通过自我推荐和上一届裁判节点中选出候选节点.裁判节点对候选节点分别按工作量、储币量、在线时长打分，并按既定权重对候选代表节点重新排序.除去黑名单节点；依次选出 200 个节点，作为代表节点.

Table 2 Three types of referee node weights

表 2 三类裁判节点权重

裁判节点类别	工作量裁判节点	权益裁判节点	见证人节点
权重比例	5	3	2

该共识机制中的裁判节点选取代表节点时，分别就该节点的工作量、储币量、在线时长等项目指标进行

评分.各项目指标所占的权重，如表 3 所示.

Table 3 Project indicator weight

表 3 项目指标权重

项目指标	工作量	储币量	在线时长
权重比例	6	2	2

组合特征加权矩阵选取代表节点，以下加权矩阵：

$$[r_1 \quad r_2 \quad r_3]\begin{bmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{bmatrix}\begin{bmatrix} R_1 \\ R_2 \\ R_3 \end{bmatrix} = M_x$$

其中：r_i i=1,2,3 代表项目指标权重；

R_j j=1,2,3 代表裁判节点权重；

m_kl k=1,2,3 ;l=1,2,3 代表 l 裁判节点对 k 项目指标的评分；

M_x 代表 x 节点的最终评分.

(3) 组合特征双重加权共识机制实现共识.系统生成新的交易，该节点向全网进行广播寻求得到足够多的确认反馈.代表节点收到请求，对交易进行验证；90%以上代表节点签名通过该交易；该交易以区块的形式记入区块链.组合特征双重加权共识机制旨在提出如何依据公平、公正的原则选出具有决策权的裁判节点、代表节点，按权重投票选取代表节点代替全网挖矿，减少了资源的浪费，同时，该共识机制对代表节点进行了一定的限制，代表节点只有投票权，无权修改交易信息，在一定程度上避免了区块链分叉的产生.

3 早期共识机制研究

区块链技术是一种基于分布式的、完全去中心化的底层结构的构架[12]，分布式系统中往往存在部分节点出现故障无法正常通信、网络阻塞或者中断、错误的信息传播等问题，这类问题被称为拜占庭将军问题[13]，Castro M[14]等人于 2002 年提出了一种实用的拜占庭容错系统[9]，该系统依赖于一致性协议、检查点协议等来保障其有序运行，Ongaro[15]博士等于 2014 年提出 Raft 协议，应用于不需要解决拜占庭将军问题的分布式系统.区块链分为公有链、私有链、联盟链等[16]，公有区块链大多采用工作量证明机制（POW）和权益证明机制（POS）[17]，私有区块链多采用变种权益和活动频率证明（POSV）[18]、行动证明（POA）[19]、股份授权证明（DPOS）[20]等达成节点间共识.其中，工作量证明（POW）机制的典型应用是比特币的共识机制，系统中所有节点处于相同的地位，各节点依靠其计算能力解决某个难度可控的数学难题，优先做出准确解答的节点获得本次活动记账权，三种典型的共识机制重要参数比较见表 4.

Table 4 Comparison of important parameters of three typical consensus mechanisms

表 4 三种典型的共识机制重要参数比较

名称	POW	POS	DPOS
记账权竞争	计算机算力（CPU、GPU）	计算机算力；节点权益结余	节点权益；引入见证人节点
挖矿成本	电力资源；时间成本	电力资源；储币量；币龄	保证金
性能效率	10min/块	10min/块	10s/块
安全威胁	51%攻击问题	节点离线时间计入币龄测算	候选人为了得到记账权作弊
面临问题	浪费资源；交易确认时间过长	鼓励屯币行为，易引发分叉	少数人操纵系统
典型应用	Bitcoin	Peercoin	Bitshare

4 总结和展望

本文主要研究区块链技术的核心技术之一共识机制，探讨了目前几种流行的共识机制，本文着重阐述了

POW、POS、DPOS 三种共识机制的原理，通过对几种共识机制的对比分析，总结了现有的共识机制存在不同的优缺点，在实际应用过程中，要做到针对不同的场景应用不同的共识机制，未来的发展趋势是将几种共识机制取长避短结合使用，在保证分布式系统安全稳定的同时，以尽量少的资源消耗，更快的达成共识.阐述了几种共识机制的优点以及存在的问题，并提出了一种改良的方案，有效地改良了工作量证明（POW）机制在资源浪费和 51%攻击等方面问题，并且引入了权益证明（POS）机制中的权益证明概念，经论证组合特征双重加权共识机制在节约资源、提高效率、保障系统安全性等方面有一定改进.未来共识机制的发展方向可能是将工作量证明（POW）和权益证明（POS）相结合.

References:

[1] Xia Qing, Zhang Fengjun, Zuo Chun. A Summary of the Consensus Mechanism of Encrypted Digital Currency System[J]. Computer systems and applications, 2017, 26(4):1-8.

[2] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.

[3] Reed S L. Bitcoin Cooperative Proof-of-Stake[J].Computer Science,2014

[4] Larimer D. Delegated Proof-of-stake white paper [online], available:http://www.bts.hk/dpos-baipishu.html.2014

[5] Xin Yunwei, Liao Dachun, Lu Guizhang. The principle, implementation and application of one-way hash function in cryptography[J]. Application Research of Computers, 2002, 19(2):25-27.

[6] Courtois N T, Grajek M, Naik R. Optimizing SHA256 in BitcoinMining[M]// Cryptography and Security Systems. Springer Berlin Heidelberg, 2014:131-144.

[7] Bentov I, Gabizon A, Mizrahi A. CryptocurrenciesWithout Proof of Work[C]// International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2016:142-157.

[8] Yuan Yong, Wang Feiyue. Development Status and Prospects of Blockchain Technology[J]. Acta Automatica Sinica, 2016, 42(4):481-494.

[9] Ministry of Industry and Information Technology, China's blockchain technology and application development white paper.

[10] Bellare M, Rogaway P. Optimal asymmetric encryption[C]// The Workshop on the Theory & Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1994:92-111.

[11] Atzei N, Bartoletti M, Cimoli T. A Survey of Attacks on Ethereum Smart Contracts (SoK)[C]// International Conference on Principles of Security and Trust. Springer, Berlin, Heidelberg, 2017:164-186.

[12] Zou Jun, Blockchain Technical Guide[M]. Beijing: Mechanical Industry Press, 2016:109-128.

[13] Lamport L, Shostak R, Pease M. The Byzantine Generals Problem[J]. Acm Transactions on Programming Languages & Systems, 2016,4(3):382-401.

[14] Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery[M]. ACM, 2002.

[15] Ongaro D, Ousterhout J. In search of an understandable consensus algorithm[J]. Draft of October, 2014.

[16] Swan M. Blockchain: Blueprint for a New Economy[M]// Blockchain : blueprint for a new economy. O'Reilly, 2015.

[17] King S, Nadal S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake[J]. 2012.

[18] Ren L. Proof of Stake Velocity: Building the Social Currency of the Digital Age[J]. 2014

[19] Bentov I, Lee C, Mizrahi A, et al. Proof of Activity[J]. AcmSigmetrics Performance Evaluation Review, 2014, 42(3):34-37.

[20] Wood G. Ethereum: A secure decentralized generalized transaction ledger. Ethereum Project Yellow Paper, 2014.

附中文参考文献:

[1] 夏清, 张凤军, 左春. 加密数字货币系统共识机制综述[J]. 计算机系统应用, 2017, 26(4):1-8.

[5] 辛运帏, 廖大春, 卢桂章. 单向散列函数的原理、实现和在密码学中的应用[J]. 计算机应用研究, 2002, 19(2):25-27.

[8] 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.

[12] 邹均，区块链技术指南[M]. 北京：机械工业出版社，2016:109-128.

金梦雪（1991-），女，山东淄博人，青岛大学数据科学与软件工程学院硕士研究生，主要研究领域为区块链隐私保护和共识机制。
通信地址：山东省青岛市市南区宁夏路 308 号，266071，
电话：13954280669，邮箱：13954280669@163.com

高鹏翔（1965-），男，高鹏翔，男，山东省莱西人，青岛大学数据科学与软件工程学院院长、教授。东北大学硕士，美国明尼苏达大学作访问学者，1995-1996 年于清华大学 CIMS 中心做访问学者，参加了国家 CIMS 设计与开发工作。主要研究领域为区块链隐私保护和共识机制，企业智能信息系统，电子商务与现代物流技术，嵌入式系统与机器人技术等，在国内外期刊发表论文 50 余篇，编著书 3 本，主持和参与教学、科学研究项目 10 余项、科研经费 400 多万元，获奖 8 项。