文章编号：2095-2163(2023)08-0175-05 中图分类号：G203；TP399 文献标志码：A

基于改进型 PBFT 共识算法的区块链高校精准资助认证模型

王 慧[1]，王 蕾[1]，郭博建[2]
（1 甘肃建筑职业技术学院，兰州 730050；2 北京华晟经世信息技术股份有限公司，北京 101100）

摘 要：为解决高校学生资助认证过程困难、信息篡改失真、信息存储中心化等问题，本文提出一种基于实用拜占庭容错算法（Practical Byzantine Fault Tolerance，PBFT）的区块链高校学生资助认证模型，将联盟链与星际文件系统（InterPlanetary File System，IPFS）相结合，实现高校学生资助认证信息存储安全可靠、认证过程留痕、信息篡改可追溯。针对传统 PBFT 算法中主节点选取无法剔除拜占庭节点的问题，本文通过节点动态评价模型改进 PBFT 算法，有效地避免了拜占庭节点成为主节点，提高了共识效率及算法性能。

关键词：联盟链；资助认证；实用拜占庭容错；星际文件系统

College student subsidy certification model using blockchain based on improved PBFT

WANG Hui[1], WANG Lei[1], GUO Bojian[2]
(1 Gansu Vocational College of Architecture, Lanzhou 730050, China;
2 Beijing HuashengJingshi Information Technology Co., Ltd., Beijing 101100, China)

【Abstract】 In order to solve the problems of college student subsidy authentication process difficulty, distortion of information tampering and centralization of information storage, this paper proposes a college student subsidy authentication model using blockchain based on Practical Byzantine Fault Tolerance (PBFT). By combining the consortium blockchain with the InterPlanetary File System (IPFS), the information storage of college student subsidy authentication is safe and reliable, the traces left in the authentication process, and the information tampering can be traced. In view of the problem that Byzantine nodes cannot be eliminated in the main node selection of traditional PBFT algorithm, this paper improves the PBFT algorithm by node dynamic evaluation model, effectively avoiding Byzantine nodes becoming the main node, improving the consensus efficiency and algorithm performance.

【Key words】 consortium blockchain; subsidy certification; practical Byzantine fault tolerance; InterPlanetary File System

0 引 言

近几年，随着高校学生数量的增长，政府对高校学生资助认定信息的可信度及安全性成了高校关注的重点。时下，大部分高校都将数据集中化地存储在本地数据库中，但在当前环境下，依然存在资助申请信息造假、信息泄露以及服务器宕机等问题，从而无法保证资助认定信息的可信度和数据存储的完整性，即使得准确、快速地核实资助认定信息的需求将很难得到满足。为此，有效保证高校学生资助认定信息的真实性、安全性和完整性成了高校管理者研究的重点。

随着区块链技术的不断发展，区块链的去中心化、安全性强、可溯源等优势对高校学生资助认定具有重大意义。近几年，区块链也从 1.0 飞速发展到 3.0，其应用场景也不断丰富起来，区块链已经应用到金融[1-2]、医疗[3-4]、农业[5-6]、游戏[7-8]、食品安全[9-10]等各个领域。区块链将密码学、共识算法、智能合约等技术进行融合，很好地实现了在互不信任的环境下对同一交易达成共识。

作为区块链的核心算法之一，共识算法可以使节点之间达成一致性协议，有助于区块链安全稳定的运行。常用的共识算法有工作量证明算法、股权权益证明算法以及 PBFT 算法等。其中，PBFT 算法

基金项目：甘肃省 2023 年高校教师创新基金项目(2023B-338)。

作者简介：王 慧(1982-)，女，讲师，主要研究方向：思想政治教育、教育信息化；王 蕾(1988-)，女，讲师，主要研究方向：思想政治教育、教育信息化；郭博建(1982-)，男，中级经济师，主要研究方向：教育信息化、企业数字化转型。

收稿日期：2023-01-13

存在共识效率低、通信压力大等问题。为了解决上述问题,本文提出一种基于改进型 PBFT 共识算法的区块链高校学生资助认定模型。

1 基于动态评价模型的 PBFT 共识算法

1.1 传统 PBFT 算法

PBFT 算法是为了解决拜占庭将军问题,也就是保证存在拜占庭节点恶意攻击时,全网节点仍能达成一致性共识,保持交易稳定进行。但 PBFT 的容错率只有 1/3,也就是整个网络中的拜占庭节点数不能超过总节点的 1/3,如果拜占庭节点数超过总节点的 1/3,那么就很难使正常节点达成共识。而且 PBFT 采用预准备、准备、提交的三段式通信,当全网节点数较多时,通信压力会很大,导致共识时延增大,影响共识效率。PBFT 主节点的选取随机性太强,不可避免拜占庭节点成为主节点,需要多次切换视图,不仅严重浪费通信成本,而且造成共识效率下降,系统可用性变差。PBFT 共识算法通信流程如图 1 所示。

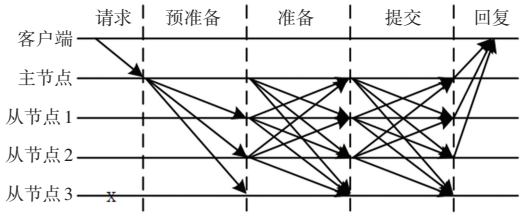

图 1 PBFT 共识算法通信流程

Fig. 1 PBFT consensus algorithm communication process

1.2 改进型 PBFT 共识算法

针对传统 PBFT 算法主节点选取无法剔除拜占庭节点,本文提出基于 PBFT 算法的节点动态评价模型,可以通过节点整体历史信任度筛选出共识节点集合参加主节点选举,有效地避免了拜占庭节点成为主节点,提高了共识效率。

1.2.1 动态评价模型

信任度模型是指参与共识的节点之间可以通过彼此的历史共识行为进行信任度评价,相互通信的节点之间可以进行标记,节点 n 在参与历史共识时能够按时、准确地向节点 m 传递消息,则节点 n 标记为有效节点,共识行为为有效行为;若节点 n 未在规定时间内向节点 m 传递消息,或者节点 m 接收的消息有缺失,或节点 n 拒绝接收节点 m 的消息,则节点 n 视为宕机节点,其行为为宕机行为;如果节点 n 在共识过程中向节点 m 传递的信息与向其它节点传递的信息不一致,则节点 n 标记为恶意节点,其行为视作恶意行为。恶意节点的标记在后续的节点互评中将无法更改。动态评价模型主要受节点往期信任度和节点近期信任度影响。对此拟做研究分述如下。

(1)节点整体历史信任度计算。节点整体历史信任度值可以通过节点参与共识的历史行为得出,主要由往期信任度值和近期信任度值计算,其中近期信任度值是评价整体历史信任度值的关键指标。往期信任度值主要体现的是节点参与上一轮共识之前的信任度,可以衡量节点在共识过程的参与程度及预测节点在接下来的共识中的活跃度。节点 i 的往期信任度 $P(i)$ 可以表示为:

$$P(i) = \sum_{j=1}^{m-1} s_j(i) - ke_j(i) \tag{1}$$

其中,m 为节点 i 共识总次数;$s_j(i)$ 为节点 i 参与第 j 次共识的有效行为标识,第 j 次共识为有效行为则 $s_j(i)$ 为 1,否则为 0;$e_j(i)$ 为节点 i 参与第 j 次共识的恶意行为标识,若第 j 次共识行为为恶意行为则 $e_j(i)$ 为 1,否则为 0;k 为恶意行为惩罚因子。

在节点整体历史信任度模型建立过程中,主要考虑节点上一轮共识表现,即节点的近期信任度值。将上一轮共识表现量化建模可以得出节点 i 的近期信任度 $L(i)$ 为:

$$L(i) = s_m(i) - d_m(i) - k^2 e_m(i) \tag{2}$$

其中,m 为节点 i 共识总次数;$d_m(i)$ 为节点 i 参与第 m 次共识的宕机行为标识,若第 m 次共识行为为宕机行为则 $d_m(i)$ 为 1,否则为 0;其余参数上述已说明,不再赘述。

根据前述往期信任度值和近期信任度可以确定出节点 i 的整体历史信任度 $Q(i)$:

$$Q(i) = xP(i) + yL(i)$$
$$x,y \in (0,1) \cap x + y = 1 \cap x < y \tag{3}$$

其中,$P(i)$ 为节点 i 的往期信任度值;$L(i)$ 为节点 i 的近期信任度值;x 为往期信任度权重因子;y 为近期信任度权重因子;权重因子的取值范围为 $(0,1)$,且 $x + y = 1$。权重因子越大,表示对应的往期信任度或近期信任度就越重要,x 越大说明参与共识的节点集合中往期信任度高的节点较多,往期信任度往往可以反映节点的可信度,但 x 过高会导致节点选举的公平性,出现垄断行为,因此往期信任度权重因子的选取应满足 $x < y$。

节点整体历史信任度作为节点参与主节点选举和共识过程的重要指标,能够实现对共识过程中的有效节点进行奖励,对宕机节点和恶意节点进行惩罚,且恶意节点的惩罚呈现指数级,即恶意行为的出

现对节点整体历史信任度值的影响极大。整体信任度也成为视图更新后，节点动态评价模型建立的重要依据。

(2)节点动态评价模型建立。在每次视图更新后需要对所有节点的信任度进行更新，更新操作主要是基于整体历史信任度和节点初始化信任度。节点 i 的动态评价模型如下：

$$M(i) = H_{init} + Q(i) \tag{4}$$

其中，$M(i)$ 表示节点 i 更新后的动态信任度值；H_{init} 为节点的初始化信任度；$Q(i)$ 为节点的整体历史信任度值。节点动态评价模型可以作为节点等级划分的重要依据，通过为评价模型设置不同阈值区分节点等级，并为不同等级设置不同行为，从而提升共识效率，减少通信损耗。

1.2.2　评价等级划分

为了优化主节点选举方式，提升共识效率和系统安全性，根据上述节点评价模型计算的动态信任度值，设置不同阈值区间，划分节点评价等级为共识节点集合 N_c、辅助节点集合 N_a 以及同步节点集合 N_s。各个节点集合分别表示为：

$$N_c = \{M_i \mid M_i > M_g\} \tag{5}$$

$$N_a = \{M_i \mid M_g > M_i > M_s\} \tag{6}$$

$$N_s = \{M_i \mid M_s > M_i\} \tag{7}$$

这里，M_g 为共识节点集合阈值，将动态信用度值 $M_i > M_g$ 的节点集合设置为共识节点集合 N_c。节点信任度值满足 $M_s < M_i < M_g$ 的节点集合设置为辅助节点集合 N_a，其中 M_s 为辅助节点集合阈值。最后，把信任度值满足 $M_i < M_s$ 的节点集合设置为同步节点集合 N_s。选择共识节点集合中信任度值最大的节点作为主节点，且集合中的所有节点参与共识过程。辅助节点集合中的节点也参与共识过程，但不参与主节点选举。同步节点集合中的节点只负责共识信息的同步，不参与共识过程。节点等级划分及权限操作见表 1。

表 1　节点等级划分及权限

Tab. 1　Node level classification and permissions

节点等级	阈值区间	节点权限
共识节点	$M_i \in (M_g, +\infty)$	主节点选举、参与共识
辅助节点	$M_i \in [M_s, M_g]$	参与共识
同步节点	$M_i \in (-\infty, M_s)$	同步信息

1.2.3　算法整体流程

改进型 PBFT 算法通过分析节点参与历史共识的行为，构建节点动态评价模型，将节点往期信任度和近期信任度作为节点等级划分的重要依据，通过初始化阈值区间，将节点划分成有效节点集合、辅助节点集合以及恶意节点集合。节点等级划分完成后，在有效节点中进行主节点选举，选择出信任度值最高的当选为本次视图的主节点。如果判断出有恶意节点，则设置恶意节点不允许参加共识。节点标记完成后，对请求进行共识，若节点未达成一致共识，则切换视图更新节点信任度，重新进行节点等级划分。反之，则生成新的区块直至请求完成。算法整体流程图如图 2 所示。

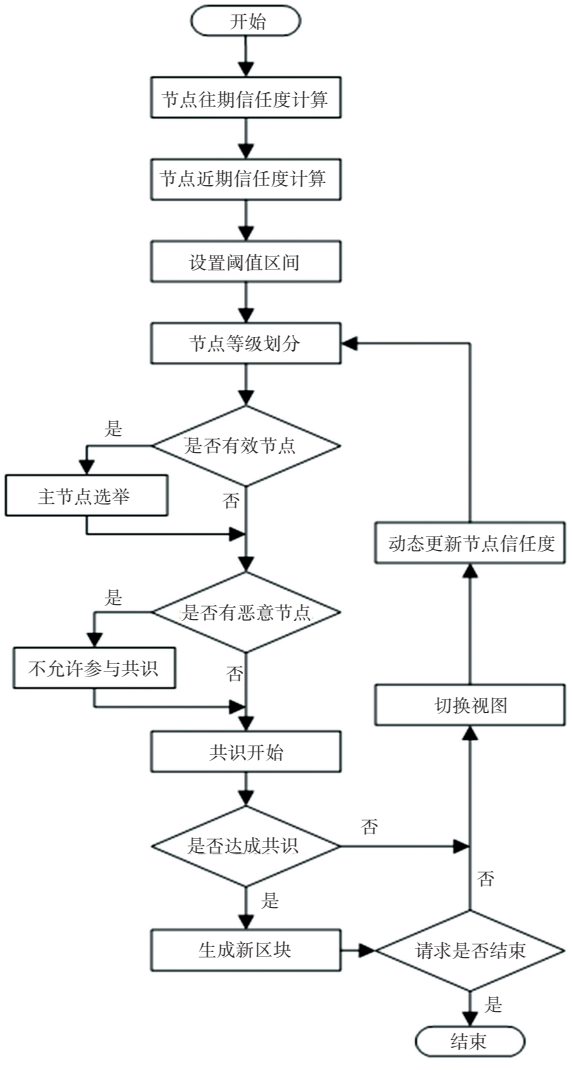

图 2　改进型 PBFT 算法流程

Fig. 2　Process of improved PBFT algorithm

2　基于联盟链的高校学生资助认证模型

2.1　模型架构设计

本文针对高校学生资助认证信息存在信息篡改失真、信息易泄露、信息存储中心化、信息存储孤岛化等问题，结合联盟区块链技术，采用改进后的 PBFT 算法，设计出数据存储安全可靠、认证过程留

痕、信息篡改可追溯的高校学生资助认证模型,以此来保证高校学生资助认证数据的真实性和完整性,提高资助认证信息的可信度。基于联盟链的高校学生资助认证模型如图 3 所示。

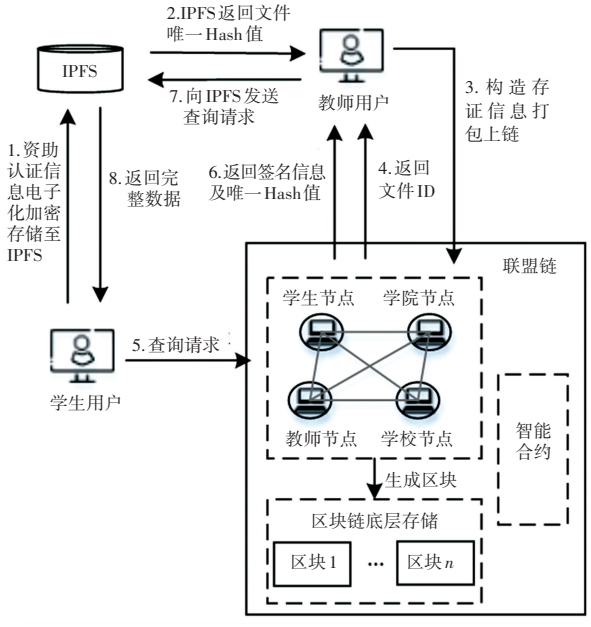

图 3 基于联盟链的高校学生资助认证模型

Fig. 3 Subsidy funding and certification model for university students based on alliance chain

为了缓解数据存储压力,链下采用 IPFS 存储数据完整信息,链上只需存储数据摘要信息。基于联盟链的高校学生资助认证模型主要用户为学生用户、教师用户、学院用户和学校用户,其中学生用户作为资助对象,需要上传和更新需要认证的信息,首先将需要认证的信息上传至 IPFS 进行存储,上传完成后 IPFS 返回文件 Hash 地址到管理员用户,管理员用户构造存证信息并打包上链,上链请求发送后各节点开始对上链信息进行共识,共识通过、则该资助认证信息上链成功再返回数据 ID 到客户端。若学生用户发起查询数据请求后依然需要各节点进行共识,共识通过即向管理员用户返回签名信息和数据唯一标识,管理员用户获取到唯一标识就会向 IPFS 发送查询请求,IPFS 接到请求则向学生用户返回需要查询的完整数据。

2.2 核心功能模块设计

2.2.1 资助认定信息上传模块

资助认定信息上传用户大多是学生用户,实现链下数据 IPFS 存储,且链上/链下数据同步更新,将 IPFS 储存产生的唯一标识打包上链,不仅链上链下数据进行关联,而且保证了唯一标识不可被篡改。具体流程如下:首先学生通过平台填写资助认定信息并提交,提交后系统校验数据格式是否合格,若不合格系统提醒学生修改。校验合格后,服务器将数据进行加密并存储在 IPFS 中,实现数据的链下存储。数据链下存储完成后,返回数据的 Hash 地址。管理员用户将返回的 Hash 地址、用户签名以及数据主键等重要属性统一打包,构造出存证信息并发送上链请求。链上主节点接收到请求后,各个共识节点发起共识,若共识成功则返回上链数据唯一标识,并向学生用户发出提醒资助认定系统上链成功。反之,返回资助信息提交页面重新修改认定信息。资助认定信息上传模块流程如图 4 所示。

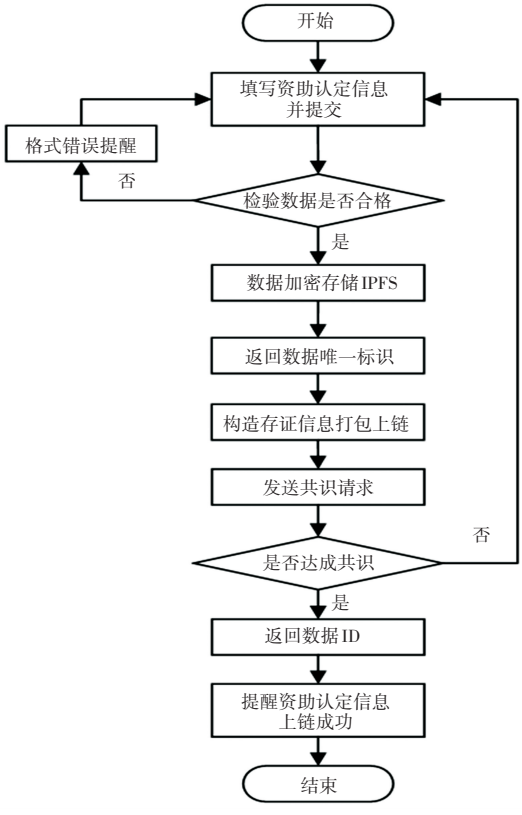

图 4 资助认定信息上传模块流程

Fig. 4 Process of uploading module for subsidy recognition information

2.2.2 资助认定信息共识模块

资助认定信息共识模块主要是对信息上链请求进行共识,主要步骤如下:首先设置节点规模、节点初始化信任度值、节点等级划分阈值等参数,然后按照一致化协议进行主节点广播交易请求,各辅助节点依次进入预准备阶段、准备阶段以及确认阶段。在每个阶段,辅助节点之间相互验证收到的共识信息,在共识时间范围内收到多数节点返回的一致信息则进入下一阶段。达成共识后,对共识信息进行密钥签名同时提醒共识成功。资助认定信息共识模块流程如图 5 所示。

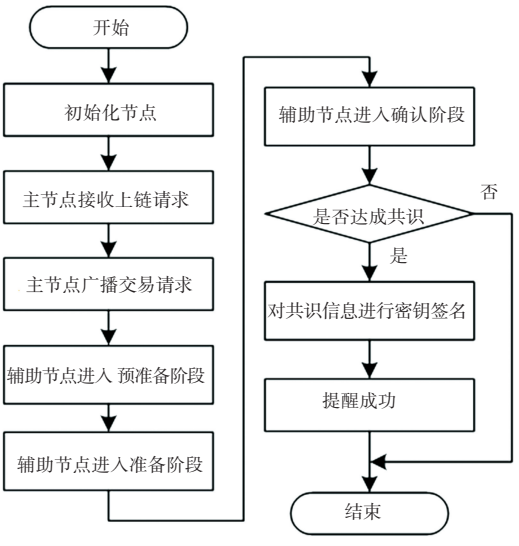

图 5　资助认定信息共识模块流程

Fig. 5　Process of the consensus module for funding recognition information

2.2.3　资助认定信息查询模块

资助认定信息查询模块主要是为不同用户提供可信的资助认定信息，主要流程如下：首先对用户的身份信息进行认证，认证通过后接收查询请求并进行共识，共识成功则向管理员返回信息 Hash 地址及查询人签名信息，然后管理员用户将文件的 Hash 地址发送到 IPFS 进行查询，IPFS 查询成功后根据签名信息向查询人返回完整的数据信息，至此整个查询流程终止。资助认定信息查询模块流程如图 6 所示。

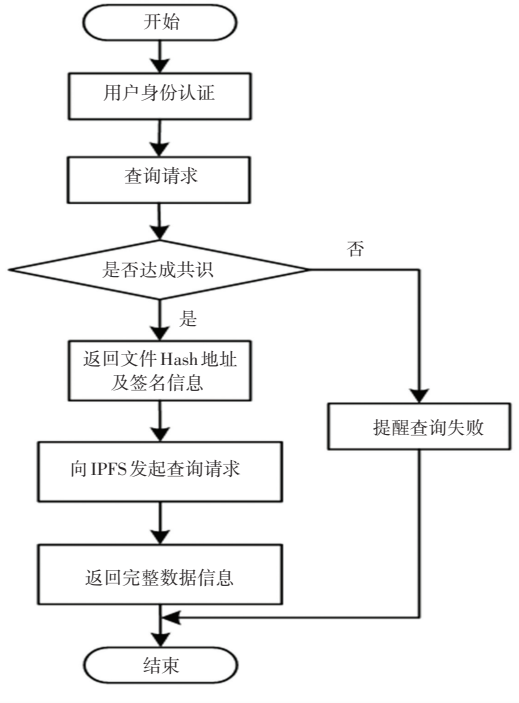

图 6　资助认定信息查询模块流程

Fig. 6　Flow of the funding confirmation information query module

3　结束语

本文提出一种基于改进型 PBFT 共识算法的区块链高校学生精准资助认定模型，通过建立动态评价模型有效地抑制了传统 PBFT 在主节点选择上的随机性，改进了共识效率的同时提升了吞吐量。高校学生资助认定模型将联盟链与 IPFS 结合起来，链下通过 IPFS 加密存储完整资助认证信息，将链下信息摘要构造成存证信息打包上链，既缓解了链上数据储存压力，又提升了数据上链效率。总体来说，基于改进型 PBFT 共识算法的区块链高校学生资助认定模型可以解决高校学生资助认证过程困难、信息篡改失真、信息存储中心化等问题，基本满足高校学生资助认证的实际需要。

参考文献

[1] 郭菊娥，陈辰. 区块链技术驱动供应链金融发展创新研究[J]. 西安交通大学学报(社会科学版)，2020，40 (03)：46-54.
[2] 夏兵，张军令. 我国银行业“区块链+供应链金融”业务的现状分析及推进建议[J]. 新金融，2020，2(10)：28-31.
[3] 张超，李强，陈子豪，等. 联盟式医疗区块链系统[J]. 自动化学报，2019，45(08)：1495-1510.
[4] 薛腾飞，傅群超，王枞，等. 基于区块链的医疗数据共享模型研究[J]. 自动化学报，2017，43(09)：1555-1562.
[5] 赵宇晨. 区块链技术在农产品供应链中的发展[J]. 电子技术与软件工程，2022 (12)：145-146.
[6] 孙道权，庄愉，孙宁苓. 区块链技术在农业领域中的应用[J]. 农业技术与装配，2020，362(02)：67-69.
[7] 徐十珍，李伟. 基于区块链的游戏资产交易平台研究[J]. 计算技术与自动化，2019，38(02)：151-156.
[8] 安金. 基于区块链技术的游戏生态系统架构研究与设计[J]. 信息与电脑(理论版)，2018(15)：56-57,60.
[9] 吴晓彤，柳平增，王志锋. 基于区块链的农产品溯源系统研究[J]. 计算机应用与软件，2021，38(05)：42-48.
[10] 刘胜艳. 基于区块链的食品安全溯源技术研究[J]. 现代食品，2022，17(05)：151-153.