文章编号：2095-2163(2022)09-0165-07 中图分类号：TP309 文献标志码：A

用于图片交易的混合共识机制

唐树均，陈世平

（上海理工大学 光电信息与计算机工程学院，上海 200093）

摘 要：随着信息技术的发展，越来越多的用户通过线上网站传输图像、浏览照片、交易版权。近年来，由于元宇宙概念逐渐引发热议，通过区块链进行的图片交易越来越多。区块链是一种分布式的数据库账本，拥有去中心化、防篡改、不依赖可信第三方等优良特性，但现有的区块链共识方案在处理图片交易时，存在奖励单一，过程复杂等不足。本文研究改进了工作量证明算法与实用拜占庭算法，并设计了基于工作积分的节点分级机制用于沟通公有链和联盟链；提出了基于双链的混合共识机制，以弥补现有共识机制在处理图片交易时节点选举随意，缺少奖惩机制的不足。实验表明，新的混合共识机制在处理图片交易时减少了通信开销，提高了交易速度。

关键词：区块链；交易；版权

Hybrid consensus mechanism for pictures trading

TANG Shujun, CHEN Shiping

(School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China)

【Abstract】With the development of information technology, more and more users transmit images, browse photos and trade copyright through online websites. In recent years, due to the hot discussion of the concept of meta universe, more and more pictures transactions are carried out through the blockchain. Blockchain is a distributed database ledger, which has excellent characteristics such as decentralization, tamper proof and independence of trusted third parties. Using blockchain technology can carry out pictures trading, but the existing blockchain consensus scheme has many deficiencies such as single reward, complex process and so on in dealing with pictures trading. This thesis studies and improves the Proof of Work mechanism and Practical Byzantine Fault Tolerance mechanism, and designs a node classification mechanism based on work integral to communicate the public chain and alliance chain. Finally, a hybrid consensus mechanism based on double chain is proposed to make up for the shortcomings of the existing consensus mechanism, such as random node election and lack of reward and punishment mechanism. Experiments show that the new hybrid consensus mechanism has the advantages of reducing communication overhead and improving transaction speed.

【Key words】blockchain; trading; copyright

0 引 言

随着元宇宙概念的迅猛推广，以图片为代表的数字媒体在网络中的应用日益广泛。作为信息密度较高的传播载体，大量图片被制作、压缩、上传、下载。相较于文字或短视频，基于图片的信息在传播时具有快捷即时、阅读方便、易于接受等优良特性。随着广告营销、电子商务、互联网自媒体的快速发展，图片版权交易也进入高速增长期，买方/卖方的数量以及整体的交易规模都在持续增长。而现有的区块链系统在处理交易时往往简单套用虚拟货币的共识机制，不能适用于图片交易。

在现有图片交易的全过程中，存在 2 种各有侧重的实际需求，一是版权登记，用户对版权数据的安全性有着较高需求，而对登记过程的耗时并不敏感；另一种是版权交易，用户在降低交易时间延迟方面有着更为迫切需求。

图片的版权登记与版权交易是图片在线交易的 2 个核心环节，尽管区块链技术可用于保护版权与处理交易[1-2]。但现有的区块链共识模型不能有效满足图片交易的 2 种需求，这就需要综合各种共识机制的优势，设计新的共识机制，从而安全快捷地实现图片在线交易。

1 共识机制与不足

区块链共识机制主要有 2 种，分别是工作量证明算法（Proof of Work，POW）与实用拜占庭算法（Practical Byzantine Fault Tolerance，PBFT）[3]。前

基金项目：国家自然科学基金(61472256，61170277)；上海理工大学科技发展基金(16KJFZ035，2017KJFZ033)。

作者简介：唐树均(1994-)，男，硕士研究生，主要研究方向：区块链技术；陈世平(1964-)，男，博士，教授，主要研究方向：网络安全、计算机网络通信。

收稿日期：2022-03-02

者安全性较高,但处理速度较慢;后者能快速处理交易,但安全性较差,不能单独提供公开的处理服务。对此拟展开探讨分析如下。

1.1 工作量证明机制

工作量证明机制是各个节点共同计算满足目标值难度的哈希函数,最先计算出满足难度目标的随机数(*nonce* 值)的节点将获得新区块的记账权,从而将新区块链接到区块链上。

POW 机制主要包括 3 个步骤:

(1)打包数据。节点链接事务池,并选取要打包的交易数据,计算交易数据哈希值,再通过默克尔树结构逐层计算出根节点值,最后形成新区块。

(2)计算 *nonce* 值。节点从 *nonce* = 0开始,不断改变 *nonce* 值,进行哈希运算,求出满足难度要求的 *nonce* 值。

(3)广播验证合法性。当节点计算出满足条件的 *nonce* 值后即获得记账权。可以将打包完成的新区块链接在区块链末尾,并向系统中的其他节点发送广播,其他节点对新区块进行验证,验证通过后将新区块链接在区块链末尾并返回确认信息。

现有的 POW 机制为了保证共识的安全可信,需要各个节点不断进行哈希计算,求得满足难度目标约束的 *nonce* 值[3]。该机制存在以下问题:

(1)大量的哈希计算消耗巨量电力,而产生的 *nonce* 值并无实际价值,造成了一定的浪费[4]。

(2)原始 POW 机制奖励过于单一,仅通过记账权奖励节点,对没有计算出有效 *nonce* 值的节点不能提供奖励。

(3)尽管节点投入大量算力参与计算,但不同节点的工作量并无数值化的衡量指标,难以对节点进行分类。

1.2 PBFT 机制

PBFT 机制通过主节点更新协议选举一个节点发起提案,称为主节点,其他节点检查主节点的提案并互相反馈检查结果,称为共识节点[5]。

PBFT 共识机制的工作原理如图 1 所示。研究中,将对图 1 中各重要部分的设计要点做出阐释分述如下。

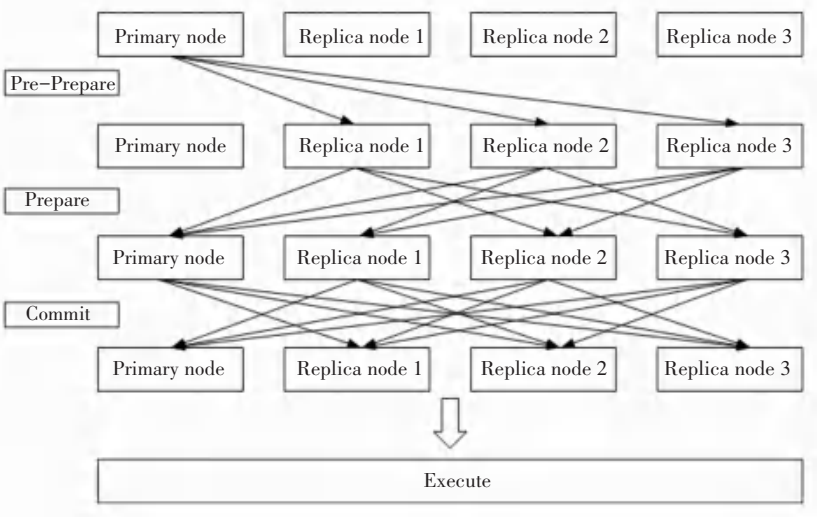

图 1 PBFT 共识机制工作原理

Fig. 1 PBFT consensus mechanism principle

(1)预准备:交易者发起图片交易,并向主节点发起交易确认请求,主节点检查请求内容并生成交易确认提案,广播到其他的共识节点。

(2)准备:系统中的每个共识节点接收主节点发出的确认提案,验证检查提案内数据的真实性,各个共识节点检查提案数据的真实性后,向其他的共识节点发送检查结果。

(3)确认:每个共识节点不断接收其他节点的检查结果,而后计算认可提案的节点数量是否满足条件,设节点总数为 n,当认可提案的节点数量超过 $2n/3$ 时,提案即被认可。

(4)执行:当足够多的共识节点确认提案后,由主节点处理提案内包含的图片交易,例如将图片交易信息写入新区块并连接到区块链末尾。

尽管 PBFT 机制能够较快地在各节点间达成共识,但该机制仍然存在以下问题:

(1)主节点选举过于随意,现有的 PBFT 机制中,主节点选举往往会在所有节点中采取轮替或随机方式,由于恶意节点可以几乎为零成本的方式成为主节点,故原始 PBFT 机制中的主节点进行虚假

交易，破坏共识过程或节点失效的可能性较高。

(2)投票过程过于复杂，给共识网络带来了过高的通信开销，当共识节点不发生拜占庭错误时，过高的通信开销会浪费大量的资源[6]。

(3)节点缺乏有效奖惩机制，不能奖励诚实节点或惩罚作恶节点，使得节点的忠诚度与积极性较低。

2　双链模型与改进 PBFT

本文改进现有的共识机制，提出一种基于双链结构的混合共识机制。

2.1　双目标 POW 机制

节点通过 POW 机制形成了去中心化的信任基础，为了描述节点在图片版权认证工作中的贡献，并以数值形式记录下来，需要改进 POW 的计算目标，建立双目标 POW 算法。考虑到哈希计算能耗较高，应当在不增加大量计算开销的情况下，改进计算方案，便于将 POW 机制的可信性拓展到共识机制的其它部分。

改进的 POW 机制仍然基于公有链系统，用于处理图片版权数据，改进后的双目标 POW 算法，区块头数据格式，可表示为：

$$head = prev \mid time \mid phash \tag{1}$$

其中，$prev$ 是前一个区块的哈希值；$time$ 是区块的时间戳；$phash$ 为图片版权数据的哈希值。

区块的计算，需用到如下计算公式：

$$SHA256(head \mid nonce) \leqslant target \tag{2}$$

其中，$head$ 为区块头数据，$nonce$ 是需要节点求解的随机值。

工作量积分计算，数学公式具体如下：

$$reverse(SHA256(head \mid nonce)) \leqslant target \tag{3}$$

其中，$reverse$ 是翻转操作，$target$ 是难度要求。

节点运行 POW 算法，从初始值开始不断增加 $nonce$ 值，反复进行哈希运算，直到求得满足目标难度约束的 $nonce$ 值。节点在不断进行哈希运算的同时，可以对比运算结果与当前目标难度值。如果求得 $nonce$ 值使结果小于等于 $target$，节点获得记账权与工作积分奖励，可以将图片的版权数据与工作积分记录打包到新区块中；如果求得 $nonce$ 值使得结果翻转后小于难度要求，节点仅获得工作积分奖励，并将工作积分记录打包到新区块中，新区块经广播由网络中的其他节点确认。

2.2　工作积分与节点分级

为了鼓励共识节点诚实工作，使用工作积分奖励诚实节点，惩罚恶意节点。以工作积分对节点分级，可以将 PBFT 机制与 POW 机制联系起来，从而提高 PBFT 机制的安全性与可信度。对此可做探讨论述如下。

(1)工作积分的认定：节点可以在公有链上处理图片版权数据，通过式(3)计算符合条件的 $nonce$ 值，从而获取工作积分，当节点获取到满足最低要求的工作积分后，可以接入联盟链，处理图片交易数据。由于工作积分的获取依赖大量哈希计算，节点工作积分的获取与扣除都储存在链上，确保节点工作积分的变动真实可信。

(2)工作积分扣除：节点参与竞选 PBFT 主节点会自动扣除一定工作积分，竞选成功可以加倍扣除工作积分，节点发生拜占庭错误也会扣除大量积分。工作积分扣除提高了恶意节点竞选主节点或破坏投票的成本，可以鼓励节点积极诚实地参与 PBFT 共识。

(3)节点分级：新加入节点直接为 C 类节点，此类节点权限较低，必须参与 POW 计算，通过式(3)获取一定工作积分后才能转换为 A 类或 B 类节点参与共识投票或竞选成为 PBFT 主节点。不同等级的节点权限各不相同，各等级节点的权限见表 1。

表 1　节点权限

Tab. 1　Node permissions

	参与图片交易	参与共识投票	竞选主节点
A 类节点	√	√	√
B 类节点	√	√	×
C 类节点	√	×	×
D 类节点	×	×	×

节点等级的转换如图 2 所示。

节点通过在图片版权认证中的诚实工作获取工作积分。按照节点的工作积分，对节点进行分级，使得工作积分较高的节点拥有较高权限，通过工作积分的获取与扣除动态调整各个节点的级别。采用节点分级与升降级策略，能够有效约束节点，提升节点的忠诚度与积极性。

2.3　改进 PBFT 算法

原始 PBFT 机制中，区块生成时间主要是待确认区块在系统中广播并获得共识所占用的时间。原始 PBFT 机制节点投票的时间复杂度为 $O(n^2)$，其中 n 为节点总数。为了排除拜占庭错误，所有节点需要互相通信 2 次，这是目前 PBFT 机制通信开销较高的主要原因。通过引入工作积分和节点分级，节点投票积极性和忠实度能够大大提高。拜占庭错

误出现的可能性大大降低。当所有共识节点都不发生拜占庭错误时,PBFT 的工作原理可以简化,如图 3 所示,主节点进行一轮准备询问,以获取其他节点状态,并直接对共识提案进行投票。在这种简易共识机制中,投票的时间复杂度为 $O(n)$,通信开销大大降低,从而减轻了系统负担,缩短了共识时间。

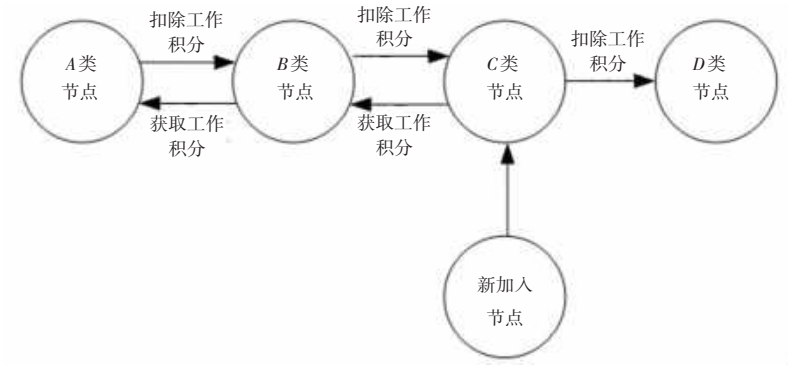

图 2 节点等级转换

Fig. 2 Node levels conversion

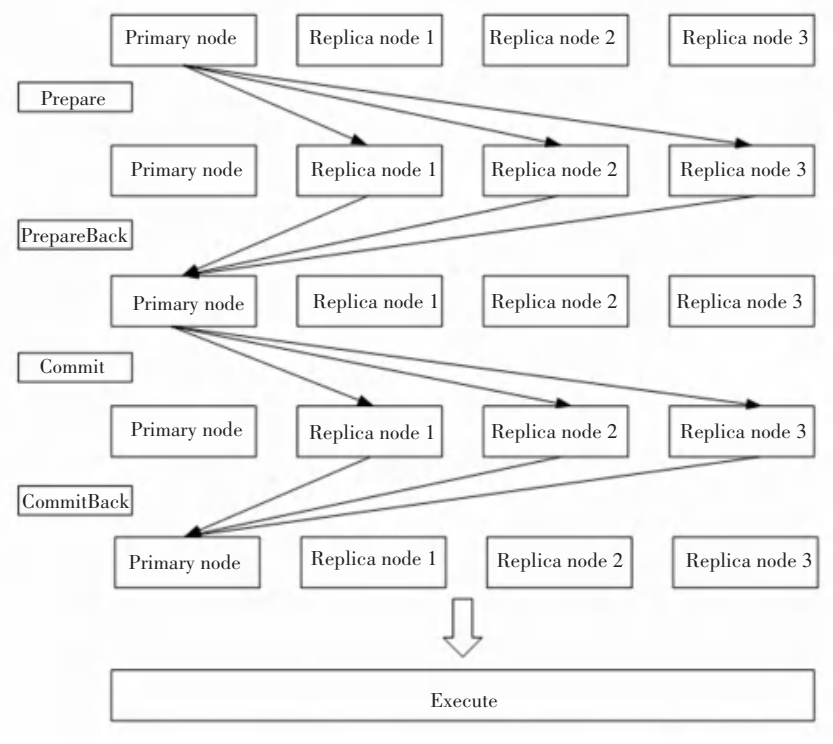

图 3 改进 PBFT 工作原理

Fig. 3 Improved PBFT working principle

改进 PBFT 机制基于联盟链部署,用于处理图片交易请求,由于简化的投票流程不考虑节点出现拜占庭错误的可能,存在一定安全风险。为提高安全性,在改进后的共识机制中,主节点首先在准备阶段获取正常在线的节点总数 m,而后在共识阶段获取票数 n。若 $n = m$ 则说明未发生拜占庭错误,主节点可以直接出块;若 $n < m$ 则共识失败,转换为原始 PBFT 机制重新进行共识。改进 PBFT 机制相当于在节点不发生拜占庭错误时进行简易投票,当节点出错几率较小时,能够有效降低通信开销。

改进 PBFT 机制中,当主节点恶意概率为 ρ_1,节点数量为 n 时,通过简易投票达成共识的通信次数为 $n(1-\rho_1)$,未能通过简易投票达成共识的通信次数为 $n(1-\rho_1)+\rho_1(n+2n^2)$,可知改进后 PBFT 投票平均通信次数为 $2n(1-\rho_1)+\rho_1(n+2n^2)$。

在原始 PBFT 机制中,当主节点恶意概率为 ρ_2,节点数量为 n 时,若主节点不是恶意节点,则通信次数为 $(n+2n^2)(1-\rho_2)$,若主节点是恶意节点,通信次数为 $(n+2n^2)(1-\rho_2)+\rho_2(n+n^2)$,则原始 PBFT 平均通信次数为 $(n+2n^2)(1-\rho_2)+2\rho_2(n+2n^2)$。

受到工作积分鼓励和节点分级的约束，可以认为 ρ_1 小于 ρ_2，因此改进的 PBFT 机制共识投票的通信次数较少。

2.4　混合共识机制

改进后的混合共识机制如图 4 所示。对图 4 中各重要组成部分，将给出研究阐述如下。

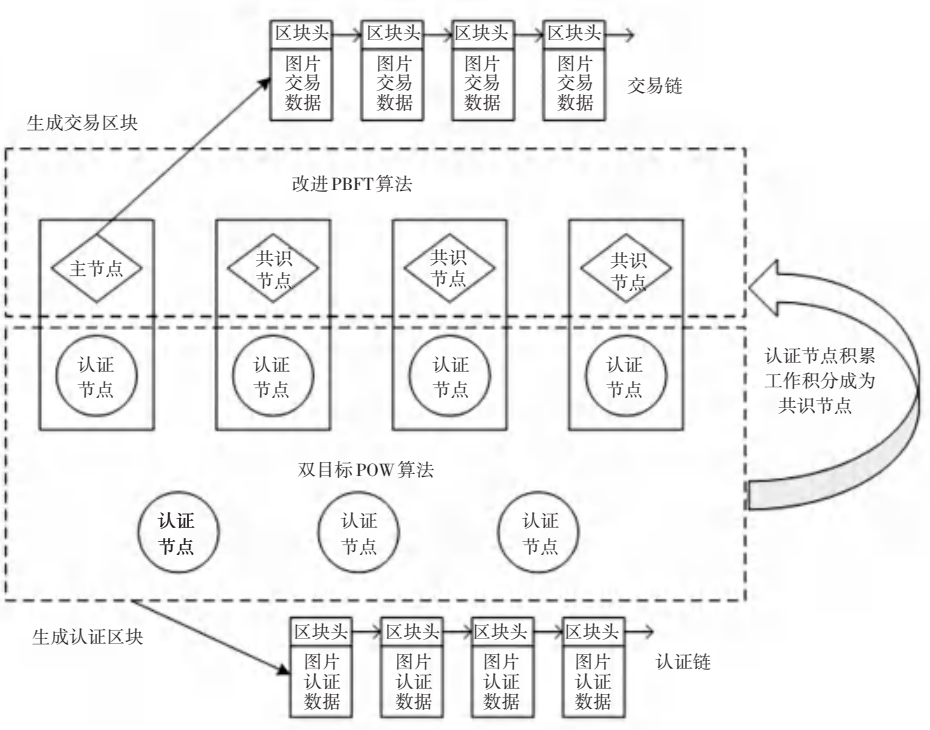

图 4　混合共识机制

Fig. 4　Mixed consensus mechanism

(1)认证节点：认证节点由普通用户构成，用户部署节点后，可以参与图片版权数据处理，通过 POW 机制检查图片版权数据，将图片版权数据打包进新区块并链接到认证链末尾。认证节点的加入和退出由各节点自由选择。

(2)主节点：认证节点积累一定工作积分后，可以经选举成为主节点，负责认证交易数据。主节点将图片交易数据打包形成新区块。

(3)共识节点：主节点广播新区块，其他参与处理图片交易数据的共识节点通过改进 PBFT 投票认可新区块，将新区块链接到交易链末尾。

(4)认证链：图片自上传至区块链系统开始，就进入图片链系统中。把图片上传视为一次特殊的交易，即通过图片的首笔交易，将图片与某一区块绑定，要求图片认证节点构造出一个新的区块记录图片版权数据，使得每张图片都按照版权登记时间顺序组成了一条由图片版权数据构成的区块链，称为认证链。认证链中除了创世区块与最新区块以外，每个交易区块都存储了指向其前一个交易区块与后一个交易区块的指针，以便于检索特定图片的版权记录。

(5)交易链：认证链负责认证图片版权，交易链负责记录图片交易，由于图片在一次认证后往往会发生多笔交易，因此认证业务较少，但需要更高的安全保障；交易链需要处理更多的交易请求，需要更短的交易确认时间。本文在认证版权时采用 POW 机制，确保版权认证过程安全可信，在处理图片交易时采用改进的 PBFT 机制，充分发挥主节点的处理能力，从而尽可能缩短交易确认时间。

2.5　主节点更新协议

为了避免主节点因意外失效导致系统故障，同时避免恶意节点拒绝工作，需要设计主节点更新协议，在主节点不能正常履行工作时激活主节点更新协议。

协议设置准备超时时间 T_1 和共识超时时间 T_2，其中 T_1 用于防止准备阶段主节点出错，T_2 用于防止共识阶段主节点出错。设节点总数为 n，则允许出错的节点数量最大为 f，其中 $n > 3f + 1$。主节点更新协议工作流程如下：

(1) 当任一共识节点在 T_1 内没有收到准备广播，或者在 T_2 内没有收到新共识，则自动激活主节点更新协议，发起主节点更新请求，并从竞选节点中选取积分最高的节点作为候选主节点，将候选主节点信息与更新请求一并广播到其他节点。

(2) 每个共识节点都持续监听广播，一旦收到

$2f+1$ 条主节点更新请求,从竞选节点中选取工作积分最高的节点作为候选主节点,并发送认可候选主节点的投票消息。

(3) 当任一共识节点收到 $2f+1$ 条投票认可自身成为主节点的投票后,即成为主节点,进行新一轮共识。

3 实验与结果

通过搭设基于双链的混合共识机制原型系统,测试改进后的混合共识机制性能与可靠性。

3.1 实验准备

文中的实验数据选用从中国知网下载的期刊封面、扉页、目录等作为实验所需要的图片,共2 000 张。

在评价指标上,关键技术的评价指标主要是处理图片交易的时间,此外还包括处理交易时节点的性能开销。实验的主要性能指标包括:时间延迟,即用户发起一次图片交易到交易完成所需时间,单位为 ms;处理速率,即在单位时间内处理用户发起交易的数量,单位为每秒处理的交易数量(tps);处理器与内存占用,即处理交易请求时电脑的硬件开销,以百分比表示。

实验中选择不同的交易发送速率,并记录在各个交易发送速率条件下,处理器和内存的占用情况,同时记录系统处理交易的速率以及各个交易从发起请求到获得确认的交易时延,将实验记录数据汇总并绘制相应实验表格。

3.2 实验结果与分析

内存占用与交易发送速率的实验结果如图 5 所示。改进 PBFT 机制相比原始 PBFT 而言没有明显的内存开销,交易发送的速率在增长到 60 tps 之前,原始 PBFT 机制和改进 PBFT 机制的内存占用都随着交易发送速率呈线性增长;当交易发送速率大于 60 tps后,2 种不同机制的内存占用增加并不明显,这是由于系统处理能力趋于饱和,额外的交易请求被不断推迟,并没有被立即处理,体现为内存占用在交易速率大于 60 tps 后,增加并不明显;在交易发送速率最大时,改进 PBFT 的内存占用较小,说明改进 PBFT 机制在一定情形下能够降低内存开销。

处理器占用与交易发送速率的实验结果如图 6 所示。改进 PBFT 机制能够降低处理器开销,交易发送的速率在增长到 60 tps 前,处理器占用随交易发送速率呈线性增长;当交易发送速率大于 60 tps 后,由于系统处理能力趋于饱和,额外的交易请求被不断推迟,并没有被立即处理,体现为交易速率大于 60 tps 后,处理器占用随交易速率增加而增加的速度有一定降低。并且,在交易发送速率大于 20 tps 时,改进 PBFT 的处理器占用比原始 PBFT 更低。

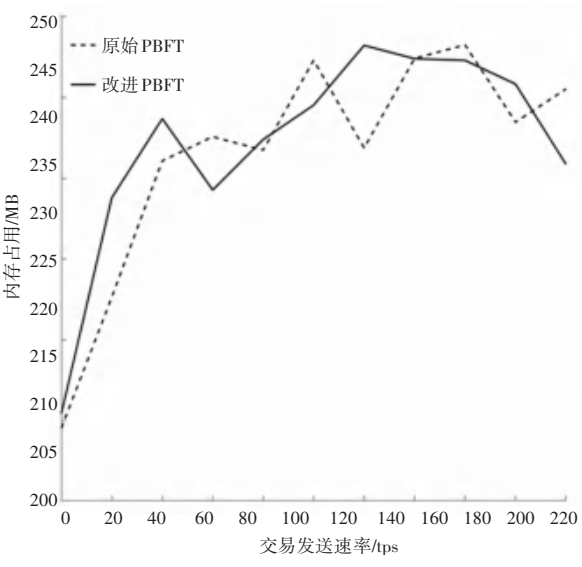

图 5 内存占用

Fig. 5 Memory occupation

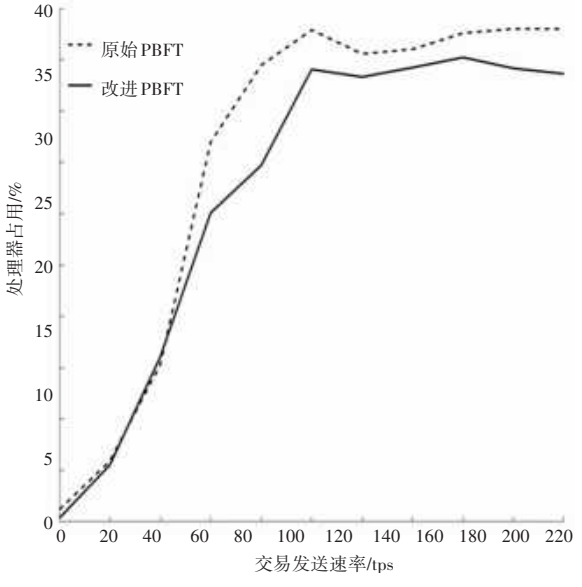

图 6 处理器占用

Fig. 6 CPU occupancy

交易处理速率与交易发送速率的实验结果如图 7 所示。改进 PBFT 机制能够提高交易处理速率上限,当前系统的交易处理能力上限在 60~70 tps 之间,交易速率高于该上限,无论采用原始 PBFT 方案或者改进 PBFT 方案,系统处理速率并不会进一步增加。改进 PBFT 和原始 PBFT 方案在交易发送交易速率为 100 tps 时都达到了最大交易处理速率。此时改进 PBFT 的交易处理速率为 71 tps,处理器占用为 25.8%,而原始 PBFT 方案的交易处理速率为

66 tps，CPU 占用为 29.8%，说明改进 PBFT 方案能够降低计算开销，占用较少资源即可达到最大交易处理速率。

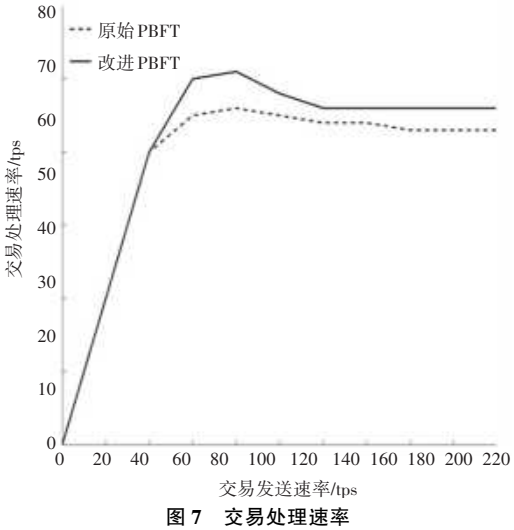

图 7　交易处理速率

Fig. 7　Transactions processing rate

交易延迟与交易发送速率的实验结果如图 8 所示。改进后的 PBFT 方案相比原始 PBFT 方案完成交易的延迟较低，与改进 PBFT 方案和原始 PBFT 方案在通信次数上的分析讨论相吻合，说明基于工作积分的改进 PBFT 方案在相同的交易处理场景下具有缩短共识时间的优势。此外，当系统的交易处理速率达到上限后继续增加交易发送量，改进的 PBFT 方案，时间延迟增幅较小，而原始 PBFT 方案的时间延迟增幅较大，进一步说明改进的 PBFT 方案在降低通信时间开销上具有一定优势。

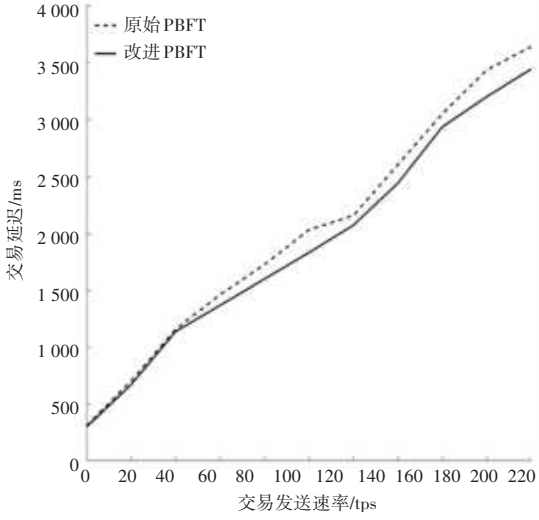

图 8　交易延迟

Fig. 8　Transactions delay

3.3　实验总结

通过对原型系统进行测试，证明了基于双链结构的混合共识机制的计算开销更小，单笔交易时间延迟更低。各主要功能正常运行，关键性能指标优于现有共识机制。随着节点和交易量的增加，系统运行正常，稳定性良好，可以进行较大规模的图片交易工作。

4　结束语

本文研究了用于图片版权交易的区块链双链模型。通过设计工作积分与节点分级，沟通了安全性强的 POW 共识机制与处理效率高的 PBFT 共识机制；基于工作积分改进了 PBFT 共识机制的投票流程，减少投票次数，从而降低投票带来的通信开销；通过搭设测试原型系统，以实验验证技术方案的可行性与技术优势。与现有的共识机制相比。本文提出的混合共识机制相比传统技术具有以下技术优势：

（1）由改进 POW 机制处理图片版权数据，由改进 PBFT 机制处理图片交易数据，相比单一的 POW 机制，有效降低认证交易数据所需的计算开销。

（2）通过工作积分有效奖励诚实节点，惩罚恶意节点；且节点分级可以将恶意节点逐步降级，最终将其排除在外。

（3）改进 PBFT 机制的通信开销与计算开销较小，处理交易数据时延迟更低。

（4）混合共识机制兼顾了 POW 机制的高可信度与 PBFT 机制的高性能，能够在同样可信的条件下，提供更快的图片交易认证服务。

但本文提出的混合共识机制仅考虑了 POW 与 PBFT，没有兼顾其他诸如股权证明（POS）和重要性证明（POI）等共识机制。随着共识机制的进一步发展，多种共识机制混合值得后续深入的系统研究。此外，本文提出的工作积分与节点分级机制，可以进一步部署在区块链系统的智能合约中，从而提供更为安全的运行环境。

参考文献

[1] 王春霈，董剑，谷博文. 区块链技术在原创作品保护系统中的应用[J]. 智能计算机与应用，2020，10(09)：25-28.

[2] 李永欣，樊重俊，安艾芝. 基于“互联网+慈善”的区块链技术在募捐领域的应用研究[J]. 智能计算机与应用，2020，10(06)：86-88，91.

[3] 邵奇峰，金澈清，张召，等. 区块链技术：架构及进展[J]. 计算机学报，2018，41(05)：969-988.

[4] 邓小鸿，王智强，李娟，等. 主流区块链共识算法对比研究[J]. 计算机应用研究，2022，39(01)：1-8.

[5] 刘懿中，刘建伟，张宗洋，等. 区块链共识机制研究综述[J]. 密码学报，2019，6(04)：395-432.

[6] 徐治理，封化民，刘飚. 一种基于信用的改进 PBFT 高效共识机制[J]. 计算机应用研究，2019，36(09)：2788-2791.