Computer Science and Application 计算机科学与应用, 2021, 11(1), 45-55
Published Online January 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.111006

Hans汉斯

分片负载的多轮均衡化验证方案

李　敏，李志淮*，白　兵，陈玉华

大连海事大学，信息科学技术学院，辽宁 大连
Email: *qhlee@dlmu.edu.cn, 1029440234@qq.com, 1285131907@qq.com, yuhuach@dlmu.edu.cn

收稿日期：2020年12月4日；录用日期：2021年1月8日；发布日期：2021年1月18日

摘　要

分片技术是区块链扩容的链上核心解决方案。针对区块链分片随机分配交易机制产生的区块链分片间负载不均衡问题，提出了一种基于节点验证能力评级的区块链分片负载的多轮均衡化验证方案。首先，根据选定的节点评级模型，对节点验证交易的能力进行评级；其次，将分片内的交易验证分为多轮，在每轮验证后，根据各分片未验证交易数对剩余负载进行判断；最后，根据各分片剩余负载，分配验证能力较高的节点到负载较大的分片进行下一轮验证。通过实验验证，本文提出的多轮均衡化验证方案，可以有效提高高负载分片的交易验证率，促进分片间负载的均衡化，优化分片的区块链链上扩容。

关键词

分片技术，交易验证率，负载均衡，节点评级，多轮验证

Multi-Round Balancing Verification Scheme for Sharding Load

Min Li, Zhihuai Li*, Bing Bai, Yuhua Chen

School of Information and Technology, Dalian Maritime University, Dalian Liaoning
Email: *qhlee@dlmu.edu.cn, 1029440234@qq.com, 1285131907@qq.com, yuhuach@dlmu.edu.cn

Received: Dec. 4th, 2020; accepted: Jan. 8th, 2021; published: Jan. 18th, 2021

Abstract

Sharding technology is the core solution for blockchain expansion. Aiming at the problem of unbalanced load among blockchain shards caused by the random distribution of transaction mechanism of blockchain shards, a multi-round balanced verification scheme of blockchain shard load based on node verification ability rating is proposed. First, according to the selected node

*通讯作者。

文章引用: 李敏, 李志淮, 白兵, 陈玉华. 分片负载的多轮均衡化验证方案[J]. 计算机科学与应用, 2021, 11(1): 45-55.
DOI: 10.12677/csa.2021.111006

rating model, the ability of the node to verify transactions is rated; second, the transaction verification within the shard is divided into multiple rounds. After each round of verification, the remaining load is calculated according to the number of unverified transactions in each shard to make judgments; finally, according to the remaining load of each shard, assign nodes with higher verification capabilities to shards with higher load for the next round of verification. Through experimental verification, the multi-round balanced verification scheme proposed in this paper can effectively improve the transaction verification rate of high-load shards, promote the balance of load among shards, and optimize the expansion of the shards on the blockchain.

Keywords

Sharding Technology, Transaction Verification Rate, Load Balancing, Node Rating, Multiple Rounds of Verification

Copyright © 2021 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

区块链作为2009年出现的比特币[1]底层技术，涉及数学、密码学、互联网和计算机编程等多个领域。区块链凭借其去中心化、不可篡改、可以追溯、集体维护、公开透明等特点，从2014年开始受到全世界的关注。从本质上来看，区块链是一个去中心化的分布式账本系统[2]，通过共识机制[3]保证数据的真实性和可靠性：区块链上的数据公开透明并且由所有参与者共同维护。随着创新应用的不断出现，区块链扩容[4] [5]成为核心难题。目前主要的扩容方案有链上扩容和链下扩容。链上扩容主要包括隔离见证[6]、分片技术[7] [8]、DAG技术[9]、增大区块等；链下扩容主要包括侧链、跨链、状态通道等。

分片技术本质上是点对点网络中分割计算能力和存储工作负载的一种分区方式。区块链分片是将网络中的节点划分为若干个相互独立的分片，单个分片只需要处理规模较少的事务，存储部分网络状态。分片间并行处理事务，从而达到区块链网络吞吐量提升的效果。在分片中，主链和分片内可以采用不同的共识算法。Elastico [10]是第一个基于分片的区块链协议，它的基本思想是将网络中的节点分成多个委员会，每个委员会在各自分片中处理不相交的交易。节点通过PoW工作量证明建立身份信息后被随机分配到各个分片中，每个分片内部独立运行BFT共识算法处理交易。Rapidchain [11]区块链协议主要包含三个阶段，分别是引导启动阶段、共识阶段和重构阶段。Rapidchain 协议首先选出一个参考委员会，由参考委员会的成员随机分配节点构成分片委员会。Rapidchain 中也使用了时代(epoch)的概念，每个时代的共识阶段可以进行多个轮次的交易验证工作，减少了委员会重构的时间。

理论上来看，区块链分片可以有效提高网络的整体性能，但是分片间的交易分配难以预先规划，分片间的负载可能不均衡，于是，某个分片内可能因为交易量过大而出现存在拥堵的现象。目前基于分片的区块链协议，尚未专门讨论分片后可能带来的各个分片间负载不均衡的问题。此外，区块链中参与验证的节点之间，实际存在较大的性能差异。在目前的验证节点分配时，往往忽略了节点间的这一差异，仅仅按照某一特定的随机分配算法进行分配。这样可能会导致各分片之间验证能力存在较大的差距。如果负载较大分片的验证能力过低、负载较小分片的验证能力过高，分片间验证效率会出现明显的失衡，严重时，整个区块链网络的交易吞吐量也会因单个分片交易验证拥堵受到影响[12] [13]。

本文针对区块链分片随机分配交易机制产生的难以预知的区块链分片间负载不均衡问题，提出了一

种基于节点验证能力评级的区块链分片负载的多轮均衡化验证方案。将分片内的交易验证分为多轮，通过轮次间的切换，获知各分片的负载；并根据选定的节点评级模型，对节点验证交易的能力进行评级；然后按照各分片剩余负载数量，分配验证能力较高的节点进行下一轮验证。该方案能够有效提高负载较大分片的交易验证率，减少出现单个分片交易拥堵的现象，实现区块链分片间负载均衡。

2. 问题的提出与分析

2.1. 分片中的交易分配与分布特点

分片技术源于传统数据库[14]领域，通过分片将数据水平分区，每个分片都保存在单独的数据库服务器上，达到负载分散的效果。区块链分片将拥有许多节点的区块链网络划分成若干个子网络，每个子网络中包含一部分节点，也就是一个分片。同时网络中的交易也会被划分到不同的分片中去处理，这样每个节点只需要处理一小部分传入的交易。不同的节点可以并行处理交易，可以增加交易处理和验证的并发度，从而提升整个网络的吞吐量。分片技术在提升吞吐量的同时也面临许多问题，例如 PoW [15]共识的单个分片 51%攻击问题、女巫攻击、分片单点过热造成的负载不均衡等。从理论上看，通过分片确实可以提升整个网络的性能，但是对于单个分片仍然可能存在单点过热问题，即分片内交易量过大导致分片拥堵。如果区块链网络中有分片处于单点过热状态的同时许多分片处于空闲状态，此时各个分片间就会出现负载不均衡的现象。

如图 1 所示。区块链网络中的交易进行随机分配后，可能会出现 1 号分片和 2 号分片中未验证交易数差距过大的现象。如果两个分片中节点处理能力恰好与 1 号分片中的交易数对应，此时 2 号分片可能会因为未验证交易数过多造成单个分片交易拥堵，2 号分片单点过热，各个分片间负载不均衡。

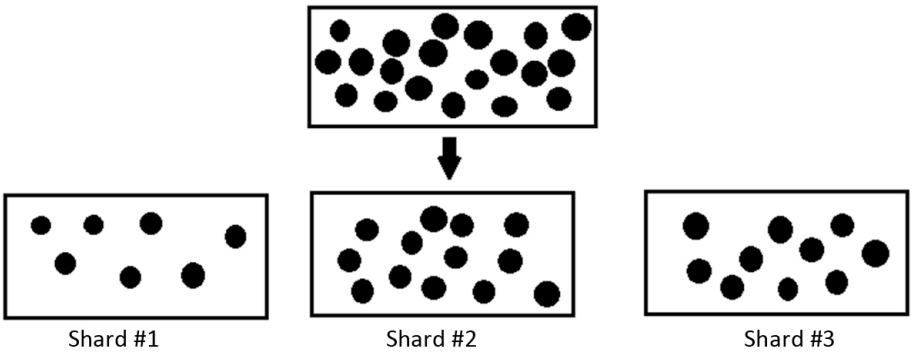

Figure 1. Unbalanced load may occur after fragmentation
图 1. 分片后可能出现负载不均衡现象

2.2. 节点的特性及其在分片间的分配

节点是区块链网络的主干，其主要作用是确认交易有效性、贡献计算资源和存储交易信息。常见的节点分配方案有：静态分配、单滚动模式、随机数模式、多滚动模式。目前大多数项目都采用随机数模式及其变体进行节点分配，随机数模式需要生成随机数，并根据随机数决定每个节点将会被分配到哪个分片中。该分配模式可以保证节点分配的公平性，但忽略了节点的性能差异，难以保证分片内的节点比例。

区块链系统中，无法预知交易的数量和大小，按照一定的原则进行分配，必然会造成交易分配不均衡现象。系统中的节点是可以预先知道的，本文在随机数模式的基础上进行改进，通过对验证节点进行调控，分配性能较高的节点到交易负载过大的分片，实施均衡化处理。

2.3. 分片间的交易负载与节点处理能力的失衡

2.3.1. 情景分析与参数设定

假设区块链系统中有 k 个分片，未验证交易集合 $T=(T_1,T_2,\cdots,T_n)$，验证节点集合 $V=(V_1,V_2,\cdots,V_m)$。未验证交易根据交易发送方地址随机分配到分片中，每个未验证交易被分配到某一特定分片的概率约为 $1/k$。假设单个分片中验证节点数目保持均匀恒定并且每一轮可验证交易的最大数量为 $T_{\max}$，我们可以运用公式(1)计算单个分片交易数为 $T_{\max}$ 的概率，其中 n 为区块链系统中的未验证交易数，x 为分配到某一分片的未验证交易数。

$$P(x=T_{\max})=\binom{1}{k}\binom{x}{n}\left(\frac{1}{k}\right)^{x}\left(1-\frac{1}{k}\right)^{n-x} \tag{1}$$

2.3.2. 失衡的概率分析

如果单个分片中的未验证交易数超过该分片中节点可验证交易的最大数量 $T_{\max}$，验证节点在短时间内无法完成验证，该分片就会交易拥堵。我们可以运用公式(2)计算单个分片中交易数超出 $T_{\max}$ 的概率。

$$P(x\geq T_{\max})=\sum_{T_{\max}}^{n}P(x=T_{\max})=\sum_{T_{\max}}^{n}\binom{1}{k}\binom{x}{n}\left(\frac{1}{k}\right)^{x}\left(1-\frac{1}{k}\right)^{n-x} \tag{2}$$

根据公式(2)，设置 $n=600$，$k=10$，用 Python 模拟计算出当交易数为 600、分片个数为 10 时，单个分片交易数分配过载的概率如表 1 所示。

Table 1. The probability of a single shard transaction allocation overload
表 1. 单个分片交易数分配过载的概率

$T_{\max}$ (分片内交易数)	P ($x\geq T_{\max}$)
80	0.052606
100	3.2e−06
120	1.9e−12
180	4.3e−41
240	3.2e−82

通过表 1 可以发现，当交易数为 600，分片个数为 10 时，单个分片等概率分配交易数超过 80 的概率约为 0.05，此时该分片的交易数已经比各分片平均分配交易多出 1/3。以以太坊[16]为例，以太坊 24 小时链上交易数在 55,000 笔左右，假设网络中的分片个数为 100 个，各分片平均分配交易则每个分片 550 笔交易。如果其中一个分片中的交易数比平均分配多出 30%，则该分片比其他分片多出 165 笔交易。可以看出，随着网络中交易数的增多，分片间所分配交易数之间的差距也会更大。

2.4. 问题的相关项目与前沿研究

由于分片技术难度较高、开发周期普遍较长，多数项目仍处于研发测试阶段。本文选取以太坊和 QuarkChain 两个分片项目进行简单介绍，分析两个项目分片方案的对分片间负载不均衡现象的相关解决方案。

2.4.1. 以太坊分片

以太坊是一个开源的有智能合约功能的公共区块链平台，通过其专用加密货币以太币提供去中心化

的以太虚拟机来处理点对点合约，是市值高达 4400 亿元、仅次于比特币的加密货币，2019 年基金会支付了 2000 万美元的开发费用。以太坊 2.0 将实现 DeFi 分片，随机分配到虚拟矿工和验证者不同的分片中，让每条分片链都拥有一个节点子集只处理和验证自己所在分片链上的交易。

但是，DeFi 分片并不意味着所有交易会均匀分布在各个分片上，仍然会有一些分片较为拥堵。

为此，Vitalik Buterin 提案在信标链中引入负载均衡的概念，通过在信标链上定义负载均衡合约，将计算负载平衡到不同的分片链上。但这种“通过相互协作的中继者实现多种不同模式的跨分片同步交易”的理念，其可靠性仍需进一步研究。

2.4.2. QuarkChain 分片

QuarkChain 是首个实现状态分片的项目，旨在用区块链技术满足全球范围商业活动的需要，通过搭建一个安全的、去中心化的、高吞吐能力的、可扩展的区块链底层技术方案，实现每秒数万级链上交易处理能力。

QuarkChain 实现负载均衡的关键是确保所有智能合约分布在所有分片上。如果网络中有成百上千个分片，则会产生一些问题。调用智能合约的用户可能需要频繁的使用跨片交易，这种情况下网络的工作效率就会大幅度降低，用户体验较差。

3. 多轮验证方案与基于节点评级的均衡化处理

3.1. 多轮方案设计思想

通过上述分析可以发现，区块链分片时随机分配交易有很大的可能会造成单个分片交易量过大、各分片间负载不均衡现象，目前一些主流的分片项目并没有针对分片间负载不均衡问题提出切实可行的解决方案。在同一个分片内，尽管增加节点数量可以提高分片的处理能力，但是会降低节点的效率，增加额外的通信开销。只有提高节点之间的通信能力，才能在保证节点效率、不增加其他开销的同时提高分片的处理能力。

因此本文提出分片负载的多轮均衡化验证方案，尝试解决目前区块链分片协议中的分片间负载不均衡的问题。首先根据节点验证交易的能力对节点进行划分，不同的交易验证能力对应不同的等级。利用多轮验证计算分片内的未确认交易数，通过分片内未确认交易数确定分片的剩余负载，分片内负载较大时，根据分片内的剩余负载确定节点调换方案，确保分片中的未确认交易在节点可验证范围内。负载较大分片的性能得到提升，分片间负载不均衡问题得到解决，区块链网络的交易吞吐量得到提升。

3.2. 节点评级模型

对节点性能进行评级，最关键的点在于如何选择合适的节点评级因素。区块链网络中节点性能指标主要包括节点生产的区块数、已处理的交易数、处理时间、完成时间等。参考 P2P 网络中对节点能力的评价方案，文献[17]从 CPU 计算能力、主存大小、网络带宽和活动时间四个方面对节点能力值进行评估。

本文对节点进行评级的主要依据是节点之前在区块链网络中的表现，根据节点验证交易的能力确定节点的性能等级。因此本文将节点 i 的生产区块数、已处理交易数、验证时间等指标综合形成一个量化值作为该节点的能力值，用符号 $P(i)$ 表示。$P(i)$ 是指节点 i 在生成微区块的过程中 1S 可验证交易的数量，是节点 i 所验证的全部交易数与该节点验证交易所花费时间总和的比值，由公式 3 计算。

$$P(i)=\frac{Count(TX_i)}{\sum_{j=1}^{N}T_j} \tag{3}$$

其中 TX_i 代表节点 i 所验证的全部交易集合。$Count$ 函数是具体数值计算函数，$Count(TX_i)$代表节点 i 所验

证的全部交易数。$\sum_{j=1}^{N} T_j$ 代表节点验证交易所花费时间的总和。节点完成每笔交易后，区块链系统自动更新交易信息，计算节点所验证的全部交易数和总花费时间，更新节点能力值。通过量化得到的节点能力值代表节点的验证能力，能力值越高，节点验证交易的能力越强，对应更高的性能等级。本文选取了大量以太坊网络中节点进行验证交易能力的评估，通过计算得出以太坊网络中节点性能的分布规律，以此作为本文节点性能划分的依据。区块链网络中交易验证能力值高于 80%节点的定义为 A 等级，能力值在 40%~80%之间的节点定义为 B 等级，低于 40%的节点以及新加入的节点定义为 C 等级。

3.3. 负载的计算模型

区块链系统中交易根据交易发送方地址随机分配，无法保证交易大小和数量分配均匀。本文方案引入多轮的思想，分片中节点达成共识打包交易出块后，计算分片内剩余负载。每一轮交易验证后都要根据分片内的剩余负载确定是否需要进行节点再分配。本文假设每笔交易的交易大小大致相同，通过计算每一轮交易验证完成后各分片中的未验证交易数判断分片内负载情况。由公式(4)计算。

$$ShardL_i = Count\left(unTX\right) \tag{4}$$

其中 $ShardL_i$ 为分片 i 的负载值，$unTX$ 为该分片某轮验证后未确认交易，$Count\left(TX_i\right)$ 代表该分片某轮验证后的未确认交易数，作为该分片剩余负载的判断依据。

通过计算每轮交易验证完成后各分片中的未验证交易数，确定该分片负载情况。节点再分配时，根据各分片的负载情况，分配性能较高的节点到负载较大的分片，实现分片间负载均衡。

3.4. 基于多轮验证的均衡化算法

VRF (Verifiable Random Function，可验证随机函数)是哈希函数与非对称加密结合的产物，可以用于区块链中出块节点的随机选择，具有快速共识、抗攻击能力高、算力需求低的优势，已应用的解决方案有 Algorand 算法和 Dfinity 中基于 BLS 的算法。每一轮验证完成后根据分片中剩余负载利用 VRF 进行节点再分配，保证节点再分配的随机性和安全性。具体步骤如下。

1) 根据公式(3)计算每个节点过去 w 轮的能力值。

2) 根据节点能力值进行节点评级。

3) 根据公式(4)计算每个分片的未确认交易，判断剩余负载。利用 VRF 随机分配评级为 A 的节点到上一轮剩余负载较大的分片中，如果有多个分片满足条件，则选择哈希值最小的分片优先分配。

4) 最后随机选取一个节点作为分片内的主节点。

交易验证开始前需要随机分配节点和交易到各个分片，首先根据随机分配算法在对应的评级里随机选取相同数目的节点进行分配，然后根据交易发送者的地址进行交易分配。节点和交易分配完成后，分片内的节点开始第一轮交易验证。一轮验证后，将完成验证并且达成共识的交易打包出块。如果一轮验证后，分片在一定时间内超时未达成共识，则直接计算分片的剩余负载，判断分片内是否含有未确认交易以及是否负载均衡。如果分片内未验证交易数和节点性能处于均衡状态，则进行下一轮验证。如果分片内未确认交易数过多，超出节点验证能力，则进行节点再分配，提高分片内节点的性能，尽快完成交易验证，将交易打包出块。分片负载的多轮均衡化验证方案的流程图如图 2 所示。

4. 实验验证与分析

为验证本文方案可以有效实现分片间负载均衡，本文设置交易验证率对比实验和轮数对比实验。随机选取以太坊网络中 2000 个节点作为实验样本数据，选用 Linux 作为实验平台，以每台服务器的不同端口模拟不同的节点，Java 语言为开发语言，实验数据用 MATLAB 进行绘制。

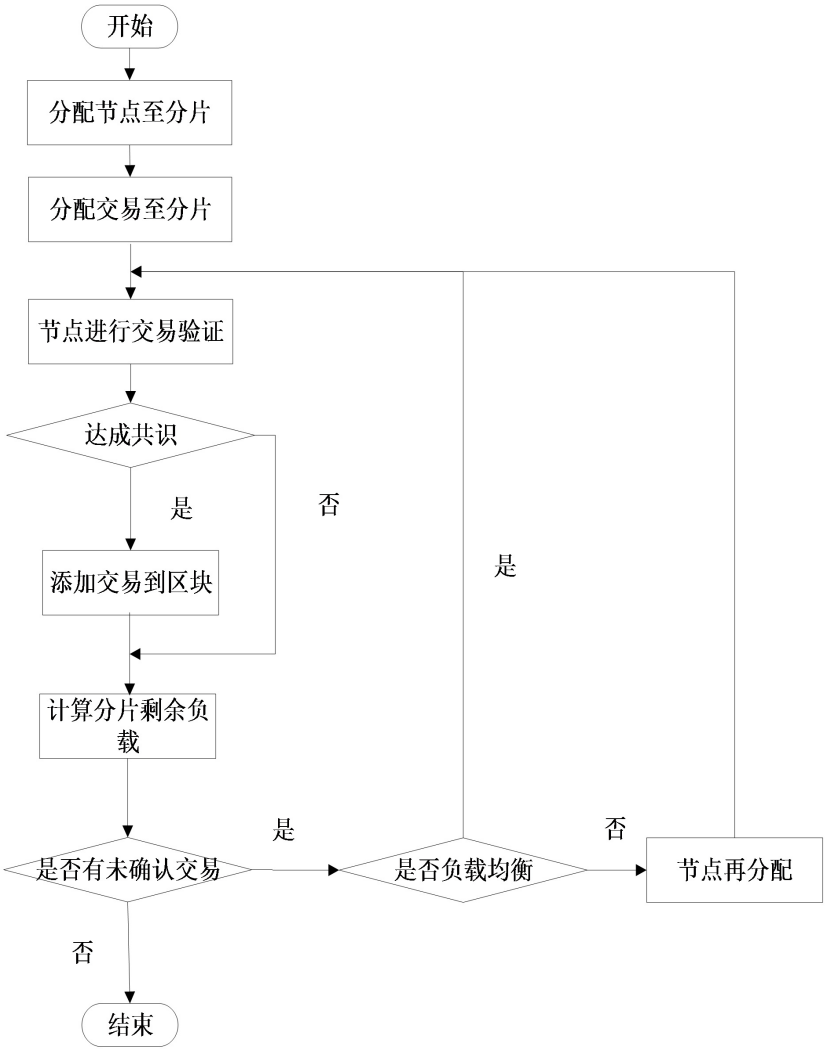

Figure 2. Flow chart of multi-round balancing verification scheme for sharding load
图 2. 分片负载的多轮均衡化验证方案流程图

4.1. 实验设计

4.1.1. 实验假设实验参数设置

本文设计的基于节点评级的多轮验证验证方案需要做以下假设：

1) 节点可以动态加入和退出，网络中节点总数保持均匀恒定。

2) 每个分片内节点数目恒定。

3) 级别相同的节点分配到每个分片的概率相同。

4) 网络中节点的通信状态良好，延迟在可控范围内。节点验证超时，则认为该节点放弃验证。

4.1.2. 实验参数设置

本文设置两个实验，对比节点性能差异对验证交易的影响。分片内采用 PBFT 共识算法，PBFT 共识算法是一种强一致性共识算法，可以容忍 1/3 的拜占庭容错率。在设置实验参数时，需要分析分片规模和分片有效性之间的关系[18]。分片失效的原因主要是分片内拜占庭节点数目过多，拜占庭节点相互沟通合谋，发送错误的消息给主节点，最终达成错误的共识。拜占庭节点合谋达成错误的共识的前提是分片

内拜占庭节点的数目大于总结点数 L 的 2/3，假设分片中的拜占庭节点数大于 2/3 L 时就会合谋，计算该分片中的拜占庭节点发生合谋的概率如公式(5)所示。其中，L 为分片内的总结点数，f 为拜占庭节点数所占比例。

$$P\left(X>\frac{2}{3}L\right)=\sum_{\left\lfloor\frac{2L}{3}\right\rfloor+1}^{L}P[X=x]=\sum_{\left\lfloor\frac{2L}{3}\right\rfloor+1}^{L}\binom{L}{x}f^{x}(1-f)^{L-x} \tag{5}$$

根据公式(5)使用 Python 模拟计算拜占庭节点所占比例 f 不同，单个分片节点数目 L 不同时，分片中拜占庭节点合谋导致分片失效的概率如表 2 所示。

Table 2. Probability of collusion of Byzantine nodes in sharding to cause shard failure
表 2. 分片中拜占庭节点合谋导致分片失效的概率

P (合谋)	$f=0.11$	$f=0.22$	$f=0.33$
$L=15$	2.5e−08	3.2e−05	1.6e−03
$L=30$	3.9e−14	2.7e−08	3.7e−05
$L=60$	1.2e−25	2.3e−14	2.4e−08
$L=90$	4.0e−37	2.2e−20	1.6e−11
$L=150$	5.0e−60	2.3e−32	9.2e−18

根据表 2 可以看出，即使在拜占庭节点比例非常高的情况下，若保证单个分片中的节点数目超过 60 个，该分片中的拜占庭节点达成合谋的概率也会低于 10^{-7}。因此本文在确定分片规模时，以该研究结果作为本文划分分片的依据，设置如下参数：总节点数目 $n=600$；每个分片中的节点数 $L=60$。

本文通过对样本数据进行计算，根据节点评级模型进行等级划分。估算在以太坊网络中，评级为 A 的节点 1S 可以验证 100 笔以上交易；评级为 B 的节点 1S 可验证 30~100 笔交易；评级为 C 的节点 1S 可验证的交易数在 30 以下。因此，本文设置三个模型进行对比实验，三个模型验证节点总数相同，均包含 A、B、C 三种等级的节点，相同等级的节点所含数目不同，对比三种模型的交易验证能力。模型 1 设置 A 等级节点 20 个，B 等级节点 20 个，C 等级节点 20 个；模型 2 设置 A 等级节点 30 个，B 等级节点 20 个，C 等级节点 10 个；模型 3 根据样本中以太坊节点验证交易的能力，随机选取节点作为对比实验。

4.2. 实验结果分析

4.2.1. 交易验证率实验

在以太坊浏览器中可以看到，目前以太坊网络中的实时未确认交易数大概在 124,700 笔，根据本文的分片规模，本实验设置每个分片内需要验证的交易总数为 15,000 笔。计算上述三种模型验证 15,000 笔交易的交易验证率，结果如图 3 所示，横坐标为每个模型验证 15,000 笔交易所需轮数，纵坐标为三个模型的交易验证率。

通过图 3 可以看出，分片内节点性能不同时，验证相同数目的交易轮数差距较大。分片内可验证交易数为 15,000 时，模型 1 采用本文方案 15 轮交易验证率约为 98%；模型 2 采用本文方案 10 轮交易验证率约为 97.5%；而模型 3 未采用本文方案 23 轮的交易验证率约为 98%。通过分析可以看出，本文提出的分片负载的多轮均衡化验证方案通过提高分片内节点的性能，分配性能较高的节点到负载较大的分片，可以有效提高负载较大分片的交易验证率，实施均衡化处理，实现各分片间负载均衡。

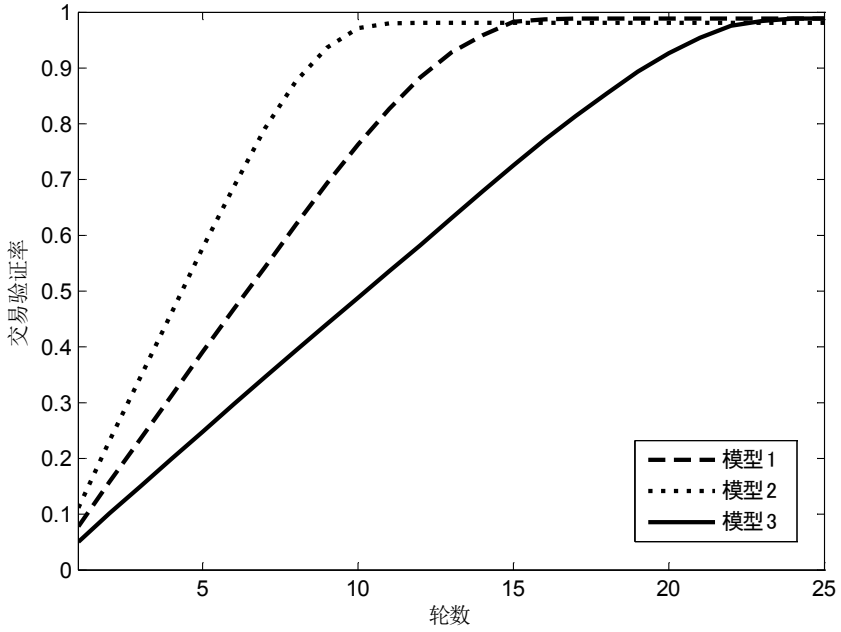

Figure 3. Transaction verification rate comparison experiment Round comparison experiment
图 3. 交易验证率对比实验

4.2.2. 轮数实验

分片中的交易是按照发送地址不均等进行分配的，每个分片中未确认交易很难达到均衡状态。本实验主要探究分片中需验证交易数不等时，不同模型验证同样数目的交易所需轮数的差别。实验设置分片内交易数分别为 5000、10,000、15,000、20,000、25,000、30,000，探究三种模型验证完成所需轮数。横坐标为分片中的交易数，纵坐标为不同模型需要的轮数。结果如图 4 所示。

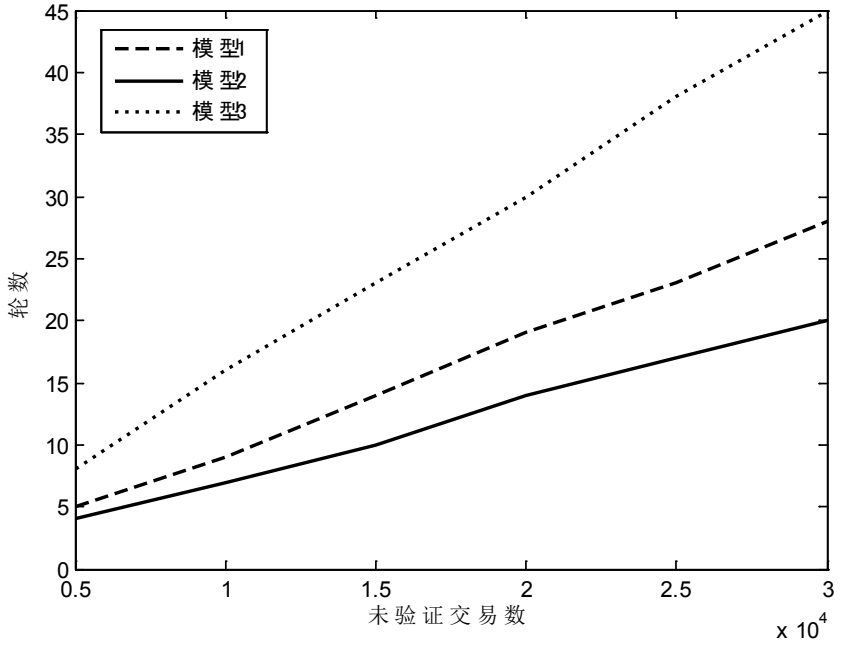

Figure 4. Round comparison experiment
图 4. 轮数对比实验

通过图 4 可以看出，不同方案验证同样数目的交易所需轮数具有很大的差别。模型 1 和模型 2 采用本文分片负载的多轮均衡化验证方案，与未采用本文方案的模型 3 相比可以更快完成验证。随着分片内交易数增多，各个方案之间的差距越来越大。假设当前分片中的节点处理能力与模型 3 大致相同，一轮验证完成后分片内剩余未确认交易数为 10,000 笔，如果不进行节点再分配，还需要 23 轮才可以完成验证；如果进行节点再分配，分配性能较高的节点到该分片，可以在 10 轮以内完成验证。通过分析可以看出，本文提出的分片负载的多轮均衡化验证方案可以有效缩短交易验证所需时间，合理分配节点，提高区块链网络的交易吞吐量。

5. 总结

本文针对区块链分片时忽略节点性能、随机分配节点造成的分片间负载不均衡的问题，提出了一种分片负载的多轮均衡化验证方案。该方案对网络中的节点进行性能评级并且划分等级，通过节点评级保证节点再分配的合理性。多轮验证不仅可以判断分片内的剩余负载，还大大减少了分片重构的时间。通过实验验证，本文方案可以有效提高负载较大分片的交易验证率，缩短交易验证的时间，实现分片间负载均衡。

本文多轮均衡化验证方案主要应用于以以太坊为代表的基于账户/余额的记账模式，上述结果表明，本文提出的多轮均衡化验证方案是可行的。但是该方案还存在不足之处，在未来的研究中需要进一步优化。首先，本文只考虑单个分片内的交易验证，下一步工作中需考虑跨分片的交易验证；其次，需要进一步分析拜占庭节点对本文方案安全性的影响，提高方案的抗攻击能力。

参考文献

[1] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. http://bitcoin.org/bitcoin.pdf

[2] 吴璨, 王小宁, 肖海力, 等. 分布式消息系统研究综述[J]. 计算机科学, 2019(B6): 1-5.

[3] 袁勇, 倪晓春. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2016, 44(11): 2011-2022.

[4] 潘晨, 刘志强, 刘振. 区块链可扩展性研究:问题与方法[J]. 计算机研究与发展, 2018, 55(10): 7-18.

[5] 喻辉, 张宗洋, 刘建伟. 比特币区块链扩容技术研究[J]. 计算机研究与发展, 2017, 54(10): 2390-2403.

[6] 常兴, 赵运磊. 比特币扩容技术的发展现状与展望[J]. 计算机应用与软件, 2019, 36(3): 55-62.

[7] Khalilov, M.C.K. and Levi, A. (2018) A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems. *IEEE Communications Surveys & Tutorials*.

[8] Li, W., Sforzin, A., Fedorov, S., *et al*. (2017) Towards Scalable and Private Industrial Blockchains. *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, Abu Dhabi, 2 April 2017, 9-14. https://doi.org/10.1145/3055518.3055531

[9] Chen, J. and Micali, S. (2019) Algorand: A Secure and Efficient Distributed Ledger. *Theoretical Computer Science*, **777**, 155-183. https://doi.org/10.1016/j.tcs.2019.02.001

[10] Luu, L., Narayanan, V., Zheng, C., *et al*. (2016) A Secure Sharding Protocol for Open Blockchains. *Proceedings of the* 2016 *ACM SIGSAC Conference on Computer and Communications Security*, Vienna, 24-28 October 2016, 17-30. https://doi.org/10.1145/2976749.2978389

[11] Zamani, M., Movahedi, M. and Raykova, M. (2018) RapidChain: Scaling Blockchain via Full Sharding. *Proceedings of the* 2018 *ACM SIGSAC Conference on Computer and Communications Security*, Toronto, 15-19 October 2018, 931-948. https://doi.org/10.1145/3243734.3243853

[12] 潘业达, 陈恭亮, 郭乃网. 区块链吞吐率提升研究[J]. 通信技术, 2019, 52(1): 134-140.

[13] 张翼. TPS 和区块链的关系以及解决方案的相关探索[J]. 中国新通信, 2018, 20(22): 70-71.

[14] 杨晶, 刘天时, 马刚. 分布式数据库数据分片与分配[J]. 现代电子技术, 2006, 29(18): 119-121.

[15] 韩璇, 刘亚敏. 区块链技术中的共识机制研究[J]. 信息网络安全, 2017, 201(9): 147-152.

[16] Wood, G. (2014) Ethereum: A Secure Decentralized Generalized Transaction Ledger. Ethereum Project Yellow Paper 151, 1-32.

[17] 任超, 李战怀, 张英. 异构 P2P 网络的分布式查询协议[J]. 电子科技大学学报, 2009, 38(1): 108-112.

[18] 王夫森, 李志淮, 田娜. 提升分片规模和有效性的多轮 PBFT 验证方案[J/OL]. 计算机工程与应用. http://kns.cnki.net/kcms/detail/11.2127.TP.20191207.0904.002.html, 2019-12-17.