网络首发时间：2023-05-11 17:04:06
网络首发地址：https://kns.cnki.net/kcms/detail/37.1389.N.20230511.1110.002.html
山东大学学报(理学版)2023 年 7 月 第 58 卷 第 7 期
Journal of Shandong University(Natural Science), Vol.58, No.7, 2023
E-mail:xblxb@ sdu.edu.cn
http://lxbwk.njournal.sdu.edu.cn
Tel:+86-531-88366917

文章编号:1671-9352(2023)07-0000-00 DOI:10.6040/j.issn.1671-9352.0.2021.681

基于边缘计算的收益激励算法对区块链分片的优化

刘云,朱鹏俊*,陈路遥,宋凯
(昆明理工大学信息工程与自动化学院,云南 昆明 650500)

摘要:在基于边缘计算的区块链中可以通过分片来提高吞吐量,但分片会降低区块链的稳定性,且同一分片内的节点可能会因距离较远增加区块传播时间,因此需要一种分片方案能够在不降低吞吐量的同时提高区块链系统的稳定性。本文提出一种收益激励(PI)算法,首先针对单个节点计算其生成一个区块的延迟和能耗,计算出该节点处理任务的最终收益;其次根据基于边缘计算的可信度模型计算出该节点的平均分片可信度,在不降低其他节点收益和平均分片可信度的同时,该节点选择能够最大化其收益的分片;最后得到所有节点收益和分片可信度均最大化的分片结构。仿真结果表明,在基于边缘计算的区块链分片中,与 OmniLedger、DBSS 和 ERCS 三种算法进行比较, PI 算法能够在保证吞吐量不降低的情况下,提高区块链系统的稳定性。

关键词:边缘计算;区块链;分片;稳定性
中图分类号:TP393 **文献标志码**:A
引用格式:刘云,朱鹏俊,陈路遥,等.基于边缘计算的收益激励算法对区块链分片的优化[J].山东大学学报(理学版),2023,58(7):0-0.

Optimization of blockchain sharding by profit incentive algorithm based on edge computing

LIU Yun, ZHU Peng-jun*, CHEN Lu-yao, SONG Kai
(Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650500, Yunnan, China)

Abstract: In the blockchain based on edge computing, the throughput can be improved by sharding, but sharding will reduce the stability of the blockchain, and the nodes in the same shard may increase the block propagation time due to the long distance, so a sharding scheme is needed to improve the stability of sharding without reducing the throughput. A Profit Incentive (PI) algorithm is proposed. Firstly, the delay and energy consumption of a block generated by a single node are calculated, and the final profit of the node is calculated according to the delay and energy consumption; Secondly, the average partition credibility of the node is calculated according to the credibility model based on edge computing; Then, the node chooses the partition that can maximize its profit without reducing the other nodes′ profit and average partition credibility; Finally, a stable sharding structure is obtained to maximize the profit of all nodes and the reliability of sharding. Simulation results show that, compared with omniledger, domain based sharding scheme and credibility based blockchain algorithm, PI algorithm can improve the stability of blockchain sharding without reducing throughput.

Key words: edge computing; blockchain; sharding; stability

0 引言

基于边缘计算的区块链系统对吞吐量和时延的要求较高,可以采用分片技术来提高区块链的可扩展性[1-2],但分片会降低区块链的稳定性,分片数越多吞吐量越高,区块链的稳定性也越差[3],且同一分片内的

收稿日期:2021-10-14
基金项目:国家自然科学基金资助项目(61761025);云南省重大科技专项计划项目资助(202002AD080002)
第一作者简介:刘云(1973—),男,副教授,研究方向为数据挖掘、区块链等.E-mail:liuyun@ kmust.edu.cn
*通信作者简介:朱鹏俊(1998—),男,硕士研究生,研究方向为区块链.E-mail:1728137634@ qq.com

节点可能会因距离较远增加区块传播时间,这就需要一种分片方案能够在基于边缘计算的区块链中,实现不降低吞吐量的同时提高区块链系统的稳定性。

Yoo 等[4]提出一种 DBSS 方案,其中基于域进行静态分片,并通过动态改变分片中的验证节点以提高区块链稳定性,但并没有考虑吞吐量问题,严重影响了系统的吞吐量。Kokoris-Kogias 等[5]提出一种 OmniLedger 方案,使用公共随机协议或加密抽签协议对验证节点进行分组,并对管理分片的节点子集进行采样和更新,实现较高的系统稳定性,但吞吐量降低较多。Kang 等[6]提出一种 ERCS 算法,构建可信度模型从可信度最高的节点中选择验证节点,并通过凸优化实现了在稍微降低吞吐量的同时仍有较高的稳定性。Yun 等[7]提出了一种基于深度 Q 网络分片的区块链(DQNSB)方案,为了保证分片方案的稳定性,估计当前恶意节点占比情况来自适应调整区块链参数,该方案具有更高的吞吐量且保持了较高的安全级别。Huang 等[8]提出一种 RepChain 方案,将信誉评分应用到区块链分片中,并提出采用交易链和信誉链的双链结构,可以在不产生过多开销的情况下对信誉评分和交易链达成共识,提高系统的吞吐量和安全级别。

为了在不降低吞吐量的同时提高区块链的稳定性,本文提出一种收益激励(profit incentive, PI)算法,首先针对单个节点计算其生成一个区块的延迟和能耗,计算出该节点处理任务的最终收益;其次根据基于边缘计算的可信度模型计算出该节点的平均分片可信度,在不降低其他节点收益和平均分片可信度的同时,该节点选择能够最大化其收益的分片;最后得到所有节点的收益和分片可信度均最大化的分片结构。

1 基于边缘计算的可信度模型

在基于边缘计算的区块链系统中,通过分片技术可以改善区块链的可扩展性,但是分片会减少参与共识的节点数,导致单个分片更容易被恶意节点攻击成功,为此使用一种多权重主观逻辑模型[6,9]来构建节点的可信度,并根据节点可信度进行分片,以提高系统的稳定性。

在一个基于边缘计算的区块链系统中构建可信度模型,包括有 M 个基站,标记为 $\mathrm{BS}_1,\cdots,\mathrm{BS}_M$,以及 N 个区块链节点,标记为 $P_1,\cdots,P_N$,节点分别为连接的边缘计算设备提供服务,如图 1 所示。

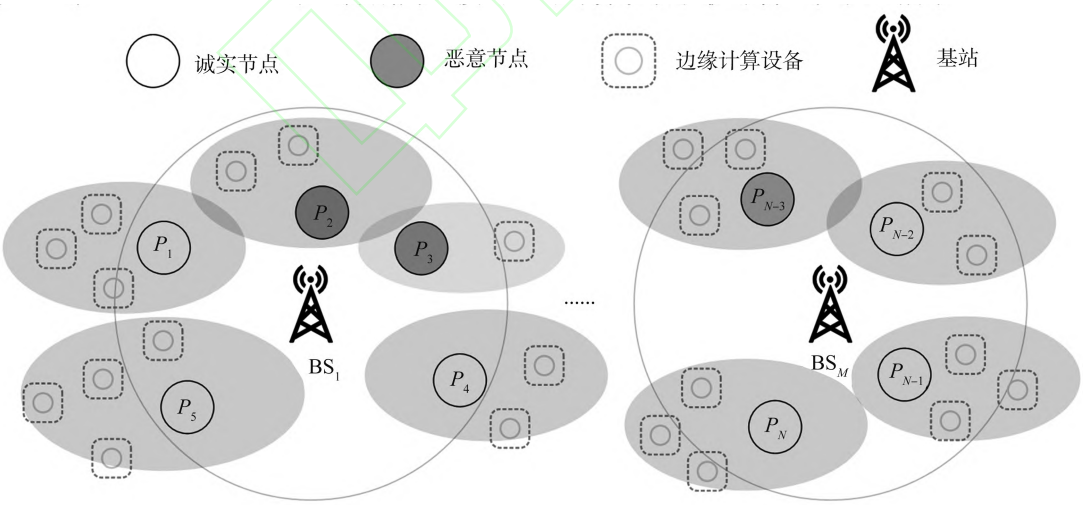

图 1 基于边缘计算的可信度模型

Fig.1 Reliability model based on edge computing

一个区块链节点的可信度除了获取其他节点的意见外,还获取该节点连接的边缘计算设备用户的意见[10]。意见是根据与该节点的互动经验得出的包括信任、不信任和不确定的判断。因此在构建可信度模型时,可以用 $o^{0\to n}=(b^{0\to n},d^{0\to n},u^{0\to n})$ 表示边缘计算设备用户对节点 P_n 的意见,其中 $b^{0\to n},d^{0\to n},u^{0\to n}$ 分别表示用户对节点的信任、不信任和不确定;用 $o^{i\to n}=(b^{i\to n},d^{i\to n},u^{i\to n})$ 表示其它节点 $i\in N\backslash\{n\}$ 对节点 P_n 的意见,其中 $b^{i\to n},d^{i\to n},u^{i\to n}$ 分别表示其它节点对节点的信任、不信任和不确定,且有 $b+d+u=1$。用户和节点在产生意见时有相同的评价标准,信任和不信任如以下所示:

$$\begin{cases} b^{s\to n}=(1-u^{s\to n})\dfrac{\chi_+^{s\to n}}{\chi_+^{s\to n}+\chi_-^{s\to n}} \\ d^{s\to n}=(1-u^{s\to n})\dfrac{\chi_-^{s\to n}}{\chi_+^{s\to n}+\chi_-^{s\to n}} \end{cases}, \tag{1}$$

其中 $s\in\{0\}\cup N\backslash\{n\}$,$\chi_+^{s\to n}$和$\chi_-^{s\to n}$分别表示用户及其他节点对节点 P_n 的正面和负面的意见总数。因此节点 P_n 的可信度 ρ^n 可为

$$\begin{aligned}\rho^n&=\omega_U\rho^{0\to n}+(1-\omega_U)\sum_{i\in N\backslash\{n\}}\rho^{i\to n}\\&=\omega_U b^{0\to n}+(1-\omega_U)\sum_{i\in N\backslash\{n\}}b^{i\to n}+\phi(\omega_U u^{0\to n}+(1-\omega_U)\sum_{i\in N\backslash\{n\}}u^{i\to n}),\end{aligned} \tag{2}$$

其中 $\rho^{0\to n}$和$\rho^{i\to n}$分别为用户和其他节点对节点 P_n 可信度的判断,$\omega_U\in[0,1]$是用户意见的占比权重;$\phi\in[0,1]$是一个给定的常数[6],表示不确定对节点可信度的影响。

节点 P_n 不仅由 ρ^n 来表征,还由节点所在分片区块确认过程的可信度$\tilde{\rho}^n$表征[11]。系统中的 N 个节点被分成 k 个分片,即形成 $\Pi=\{N_1,\cdots,N_k\}$ 的一种分片结构,其中 $N_1+\cdots+N_k=N$,且设每个分片中可以分配的最大节点数为$N_{\text{shmax}}\in[1,N]$。若节点 P_n 所在分片 k 的平均可信度 $\tilde{\rho}^n$ 为

$$\tilde{\rho}^n=\frac{\sum_{n\in N_k}\rho^n}{N_k}, \tag{3}$$

$\tilde{\rho}^n$是分片 K 确认区块过程中的可信度,$\tilde{\rho}^n$越高则对应的分片越值得信任。

在分片中需要达成共识才能将一个任务输出,在基于边缘计算的区块链系统中分片中的共识可以通过节点的加权投票达成[12],其中节点的权重与可信度成正比,即在分片 k 中节点 P_n 的投票权为

$$\omega^n(N_k|\rho)=\frac{\rho^n}{\sum_{i\in N_k}\rho^i}, \tag{4}$$

节点的可信度越高在分片中的投票权也越高。

2　收益激励(PI)算法

通过构建可信度模型可以提高区块链分片的稳定性,但是同一分片内的节点可能因为距离较远,增加了区块传播时间,降低了区块链吞吐量[11],因此提出了一种收益激励(PI)算法,在得到更高稳定性的同时保证系统的吞吐量不降低。

2.1　延迟与能耗

在进行算法之前,需要计算于边缘计算的区块链节点生成一个区块并附加到区块链上的延迟和能耗,因为节点的计算能力更差,如果延迟过高会导致节点任务丢失,降低系统的吞吐量。

节点将数据收集、处理并验证后生成区块附加到区块链的过程称为挖掘[13],将一个区块挖掘阶段记为 t。节点在进行分片后,边缘计算设备的数据需要在一个挖掘阶段 t 内被节点处理、传输并通过分片中其他节点的验证,最后生成一个区块附加到区块链上,记录该任务的节点将会获得一定的奖励 r^n,否则该任务将会被孤立并丢失。

将节点 P_n 在每个阶段 t 处理的任务定义为 $\theta_t^n=(\theta_t^{n(P)},\theta_t^{n(T)},\theta_t^{n(V)})$,其中 $\theta_t^{n(P)}$ 为任务处理所需 CPU 周期,$\theta_t^{n(T)}$ 为任务输出的大小,$\theta_t^{n(V)}$ 为任务验证所需 CPU 周期。

给定分片结构 $\Pi=\{N_1,\cdots,N_k\}$ 时,节点 P_n 的一个任务 θ_t^n 的处理延迟、传输延迟和验证延迟分别如下:

$$D^{n(P)}(\theta_t^n)=\theta_t^{n(P)}/x^n, \tag{5}$$

$$D^{n(T)}(\Pi,\theta_t^n)=\sum_{N_k\in\Pi}\frac{\beta_{n\in N_k}\theta_t^{n(T)}}{\min\limits_{i\in N_k\backslash\{n\}}R^{n,i}(l^n,l^i)}, \tag{6}$$

$$D^{n(V)}(\Pi,\theta_t^n)=\sum_{N_k\in\Pi}\beta_{n\in N_k}\max_{i\in N_k\backslash\{n\}}D^{n,i(V)}(\Pi|N_k,\theta_t^n), \tag{7}$$

其中 x^n 是节点 P_n 的计算能力,β_λ 的脚标 λ 为真时,$\beta_\lambda=1$,反之为 0;节点 P_n 在节点 P_i 的本地处理器缓冲区的验证延迟,

$$D^{n,i(V)}(N_k,\theta_t^n)=\frac{1}{x^i}(\theta_t^{i(P)}+\theta_t^{n(V)}+\frac{1}{2}\sum_{j\in N_k\backslash\{i,n\}}\theta_t^{j(V)}), \tag{8}$$

其中 l^n 为节点 P_n 的位置,$R^{n,i}$为节点 P_n 传输到节点 P_i 的速率。

节点任务传输有两种情况:1)节点 P_i 在 P_n 的范围内,通过无线链路传输;2)节点 P_i 不在 P_n 的范围内,先传输到 P_n 关联的基站,基站通过光纤链路传输到节点 P_i 关联的基站,再传输到节点 P_i。因此节点 P_n 的任务传输速率为[14],

$$\begin{aligned}R^{n,i}(l^n,l^i)&=\beta_{l^i\in R(l^n)}R_{\mathrm{PP}}^{n,i(n)}+\beta_{l^i\notin R(l^n)}\sum_{m\in M}\beta_{b^n=m}(R_{\mathrm{PP}}^{n,m(n)}+\sum_{j\in M}\beta_{b^i=j}(R_{\mathrm{PB}}^{i,j(n)}+\beta_{b^i\neq m}R_{\mathrm{BB}}^{m,j}))\\&=R^{n,i(n)}(l^n,l^i)+\beta_{l^i\notin R(l^n)}\sum_{m\in M}\sum_{j\in M}\beta_{b^n=m,b^i=j}\times(R_{\mathrm{PB}}^{i,j(n)}+\beta_{b^i\neq m}R_{\mathrm{BB}}^{m,j}),\end{aligned} \tag{9}$$

其中 $R(l^n)$为节点 P_n 的传输范围,$b^n\in M$ 表示与节点 P_n 相关联的基站;$R_{\mathrm{PP}}^{n,i(n)}$ 为节点 P_n 通过 DL 通道传输给节点 P_i 的速率,$R_{\mathrm{PB}}^{i,j(n)}$为节点 P_i 和基站 BS_j 之间的传输速率,$R_{\mathrm{BB}}^{m,j}$为基站 BS_m 和 BS_j 之间的速率。

因此节点 P_n 的任务 θ_t^n 的总延迟为 3 个延迟之和为

$$D^n(\Pi,\theta_t^n)=D^{n(P)}(\theta_t^n)+D^{n(T)}(\Pi,\theta_t^n)+D^{n(V)}(\Pi,\theta_t^n)。 \tag{10}$$

而节点 P_n 的一个任务的处理能耗、传输能耗和验证能耗的分别为 $E^{n(P)}(\Pi,\theta_t^n)$、$E^{n(T)}(\Pi,\theta_t^n)$ 和 $E^{n(V)}(\Pi,\theta_t^n)$,如下,

$$E^{n(P)}(\theta_t^n)=\vartheta^n\theta_t^{n(P)}, \tag{11}$$

$$E^{n(T)}(\Pi,\theta_t^n)=\sum_{N_k\in\Pi}\frac{\beta_{n\in N_k}p^n\theta_t^{n(T)}}{\min\limits_{i\in N_k\backslash\{n\}}R^{n,i(n)}}, \tag{12}$$

$$E^{n(V)}(\Pi,\theta_t^n)=\sum_{N_k\in\Pi}\beta_{n\in N_k}\sum_{i\in N_k\backslash\{n\}}\vartheta^n\theta_t^{i(V)}, \tag{13}$$

其中 ϑ^n 是节点 P_n 每个 CPU 周期能耗,p^n 是节点 P_n 的发射功率。则节点 P_n 的任务 θ_t^n 的总能耗为

$$E^n(\Pi,\theta_t^n)=E^{n(P)}(\theta_t^n)+E^{n(T)}(\Pi,\theta_t^n)+E^{n(V)}(\Pi,\theta_t^n)。 \tag{14}$$

通过上述计算可以得到节点完成一个任务附加到区块链的总延迟和总能耗这两个参数。

2.2 收益激励(PI)算法

根据式(10)得到的总延迟可以计算在一个挖掘阶段的时间 Δt 内任务被孤立的概率 $P_O^n(\Pi)$[15,16],

$$P_O^n(\Pi)=1-\mathrm{e}^{-D^n(\Pi)}。 \tag{15}$$

另外在区块链系统中,存在着诚实节点 N_F 和恶意节点 $N_M=N\backslash N_F$,但节点 P_n 并不知道其它节点 P_i 是否诚实,因此用 $B^{n\to i}=Pr_n\{i\in N_F\}$ 表示节点 P_n 认为 P_i 为诚实节点的概率,

$$B^{n\to i}=(1-\omega_O^n)(\omega_U^n\rho^{0\to i}+(1-\omega_U^n)\times\sum_{j\in N\backslash\{n,i\}}\rho^{j\to i})+\omega_O^n\rho^{n\to i}, \tag{16}$$

其中$\omega_O^n\in[0,1]$是节点 P_n 另一个节点意见的权重,$\omega_U^n\in[0,1]$是用户意见的权重。

因此在给定分片结构 Π 时,节点 P_n 的吞吐量 T^n 和奖励 R^n 分别为[15],

$$T^n(\Pi|B^n,\rho)=(1-P_O^n(\Pi))/\Delta t\sum_{N_k\in\Pi}\beta_{n\in N_k}\times\sum_{i\in N_k\backslash\{n\}}B^{n\to i}\omega^i(N_k|\rho), \tag{17}$$

$$R^n(\Pi|B^n,\rho)=T^n(\Pi|B^n,\rho)r^n\Delta t。 \tag{18}$$

节点 P_n 将任务附加到区块链后,最终获得的收益 V^n 为其奖励和成本之间差值,即

$$V^n(\Pi|B^n,\rho)=R^n(\Pi|B^n,\rho)-\varphi^nE^n, \tag{19}$$

其中 φ^n 是节点 P_n 的单位能量成本。

因此根据式(3)和式(19)可以得到节点 P_n 的两个参数 $\tilde{\rho}^n(\Pi)$ 和 $V^n(\Pi)$,之后将节点 P_n 从 N_k 中移动到$N_j\in\Pi\backslash\{N_k\}$中,并计算节点移动到其他分片中的 $\tilde{\rho}^n(\Pi_{k\to j})$ 和 $V^n(\Pi_{k\to j})$,若能在不降低其他节点 $i\in N\backslash\{n\}$ 的收益和平均分片可信度的同时,增加节点 P_n 在新分片中的收益和平均分片可信度,即满足式(20)—(21),则可达到节点 P_n 移动的条件。

$$\begin{cases}\tilde{\rho}^n(\Pi_{k\to j})\geqslant\rho^n(\Pi),V^n(\Pi_{k\to j})>V^n(\Pi),\\ \tilde{\rho}^i(\Pi_{k\to j})\geqslant\rho^i(\Pi)\ \text{ and }\ V^i(\Pi_{k\to j})\geqslant V^i(\Pi),\end{cases}\tag{20}$$

$$\begin{cases}\tilde{\rho}^n(\Pi_{k\to j})>\rho^n(\Pi),V^n(\Pi_{k\to j})\geqslant V^n(\Pi),\\ \tilde{\rho}^i(\Pi_{k\to j})\geqslant\rho^i(\Pi)\ \text{ and }\ V^i(\Pi_{k\to j})\geqslant V^i(\Pi)。\end{cases}\tag{21}$$

将满足上述条件的结构归为集合 $\Pi_{k(f)}$,选取节点收益和分片可信度最大的一种结构为节点 P_n 最终所在分片,

$$\arg\max_{N_j\in\Pi_k(f)}(V^n(\Pi_{k\to j}),\tilde{\rho}^n(\Pi_{k\to j})),\tag{22}$$

若节点 P_n 不存在满足式(19)或(20)的结构,则节点 P_n 不进行移动,留在原分片中。

将完成移动或达不到条件不移动的节点定义为“已访问”状态 N_v,N_v 初始值为 0,完成一个节点操作时,$N_v=N_v+1$。之后依次对未访问状态的节点进行移动,重复节点 P_n 的操作,直到 $N_v=N$ 时收益激励(PI)算法结束,最终形成一种所有节点收益最大化的稳定分片结构。

2.3　算法流程及分析

输入一种初始分片结构后,PI 算法通过不断的参数对比得出满足条件的结构,并最大化节点的收益和可信度来输出最优的分片结构,主要执行过程如下。

算法 1　收益激励(PI)算法

输入　初始分片结构 $\Pi=\{N_1,\cdots,N_k\}$

输出　最优分片结构 Π

主要步骤

Begin:

步骤 1　初始化已访问节点数 $N_V=0$;

步骤 2　Do until $N_V=N$;

步骤 3　根据式(3)和(18)计算节点$P_n\in N_k$时的 $V^n(\Pi)$和$\tilde{\rho}^n(\Pi)$;

步骤 4　P_n 移动至$N_j\in\Pi\backslash\{N_k\}$ 中,重新计算节点 P_n 的 $V^n(\Pi_{k\to j})$ 和$\tilde{\rho}^n(\Pi_{k\to j})$;

步骤 5　将所有满足公式(20)或(21)的分片结构归为集合 $\Pi_{k(f)}$;

步骤 6　最大化集合 $\Pi_{k(f)}$的值

$$\arg\max_{N_j\in\Pi_k(f)}(V^n(\Pi_{k\to j}),\tilde{\rho}^n(\Pi_{k\to j}));$$

步骤 7　设置 $\Pi\leftarrow\Pi_{k\to j}$,更新 $N_V=N_V+1$;

步骤 8　更换其他节点 $m\in N\backslash n$;

步骤 9　Loop

End

算法 1 中,步骤 6 若不存在满足条件的结构则直接跳转到步骤 8,在进行了 N 次循环后算法结束,所有节点都获得最大收益及平均分片可信度,即得到最优的分片结构。

本文从区块链系统的稳定性和吞吐量的角度,对所提出的 PI 算法的性能进行分析。基于常见的区块链稳定性定义[17],当分片中的节点均接受正确的任务输出或拒绝所有不正确的输出即保证区块链的稳定性。PI 算法中根据式(4)投票达成共识,因此只有在恶意节点的可信度高于诚实节点的可信度时才会拒绝附加正确的输出[18],即附加正确的输出 Ψ 如下,

$$\Psi=\begin{cases}1, & \sum_{i\in N_F}\rho^i\geqslant\sum_{i\in N_M}\rho^i\\ 1-\dfrac{\sum_{i\in N_M}\rho^i}{\sum_{i\in N_F}\rho^i+\sum_{i\in N_M}\rho^i}, & \sum_{i\in N_F}\rho^i<\sum_{i\in N_M}\rho^i\end{cases}\tag{23}$$

当 $\omega_U>0$ 且 $\phi>0.5$ 时,在自形成分片模型中,区块链系统的稳定性对于 $N_{\text{shmax}}=\max_{N_k\in\Pi}N_k$ 是最优的,系统分片的节点数是动态调整的,因此存在分片节点数相同和不同两种情况,此时整个系统能容忍的恶意节点数如下,

$$N-K(\max_{N_k\in\Pi}N_k+1)/2=\begin{cases}\dfrac{N-K}{2}, & \max\limits_{N_k\in\Pi}N_k=\min\limits_{N_k\in\Pi}N_k=N/K,\\ \dfrac{N}{2}\left(1-\dfrac{\min\limits_{N_k\in\Pi}N_k}{\max\limits_{N_k\in\Pi}N_k}\right), & \max\limits_{N_k\in\Pi}N_k>\min\limits_{N_k\in\Pi}N_k。\end{cases}\tag{24}$$

当恶意节点数超过系统所能容忍的最大值时,将会拒绝附加正确的输出。

分析算法的吞吐量性能可以通过系统的总吞吐量和平均块延迟[19]来体现,如式(25)-(26)分别为系统的总吞吐量和平均块延迟,

$$T(\Pi)=\sum_{n\in N}T^n(\Pi\mid B^n,\rho)\ ,\tag{25}$$

$$D(\Pi)=\frac{\sum\limits_{n\in N}D^n(\Pi,\theta_t^n)}{N}\ ,\tag{26}$$

区块链的低延迟和高吞吐量能够说明其性能更好。

3 仿真分析

3.1 仿真环境

使用 NS2 构建基于边缘计算的区块链分片仿真模型。基站数为 $M=3$ BS,3 个基站覆盖的范围圆两两相切,每个基站在带宽为 20 MHz 的单独频谱上运行,基站之间通过光纤连接。节点被随机放置在边缘计算服务范围内,每个节点配备 2.5 MHz 的带宽,并各连接 100 个边缘计算设备,包括温度、烟雾、图像和运动检测传感器等,并使用通用参数模拟[20]。基站的发射功率和覆盖范围分别为 42 dBm 和 3 000 m,节点的发射功率和覆盖范围分别为 23 dBm 和 500 m,无线链路传输参数基于 3GPP 标准。设置节点任务参数服从 Poisson 分布,其均值为 $\theta=(\theta^P,\theta^T,\theta^V)=(1\ \text{Gc},1\ \text{kb},0.5\ \text{Gc})$。规定一个挖掘阶段的持续时间 $\Delta t=5$ min,节点配备 7150N 双核服务器处理器的计算能力 $x^n=3.5$ Gc/s,16 MB L2 高速缓存和 150 W 的功耗,相比普通的区块链节点的计算能力更低,节点每能源单位的成本设置为 $\varphi^n=10^{-3}$,节点的奖励设置为 $r^n=500$。在节点意见中设定 $\phi=0.6$,$\omega_U=0.5$,ω_O^n 和 ω_U^n 遵循均值为 0.5 的泊松分布。

3.2 稳定性分析

在稳定性方面,本文将 PI 算法的性能与 OmniLedger、DBSS 算法和 ERCS3 种算法进行了比较。为了与 PI 算法提出的分片模型相比较,其他 3 种算法的分片数量被调整为 $K=N/N_{\text{shmax}}$,以便每个分片由 N_{shmax} 个节点验证输出,其中 $N_{\text{shmax}}=\max\limits_{N_k\in\Pi}N_k$ 为式(24)中的最佳值。模拟了在节点总数 $N=20$,分片的数量 $K=5$,恶意节点占比不断增加时所有算法附加的正确输出率。

如图 2 所示,随着恶意节点占比的增加,所有算法对于区块共识的附加正确输出率都降低了,但降低速率有所不同。其中 OmniLedger 和 DBSS 算法下降率是最高的,当恶意节点占比超过 25%时,附加的正确输出率迅速下降,这说明这两种算法最多只能容忍 25%的恶意节点,这是因为 DBSS 算法和 OmniLedger 只有当分片中所有节点都同意,结果才达成共识,即分片中至少有一个恶意节点时都可以拒绝正确输出。PI 算法在恶意节点占比超过 40%时开始迅速下降,说明能够容忍 40%的恶意节点数,而 ERCS 算法容忍的恶意节点数为 30%,这是因为 ERCS 算法中分片中的共识是通过常规的平均加权投票达成的,尽管验证节点是从可信度在最高的节点中选择的,但其中一些仍然可能是恶意节点,当恶意节点的数量大于诚实节点的数量,则可以拒绝附加正确的输出。在 PI 算法中每个分片内部的共识都是通过可信度加权投票达成的,只有当恶意节点的总可信度高于诚实节点的总可信度时,才会拒绝附加正确的输出,这种情况比等权投票的情况少得多。因此相比其他方案,PI 算法有更高的稳定性。

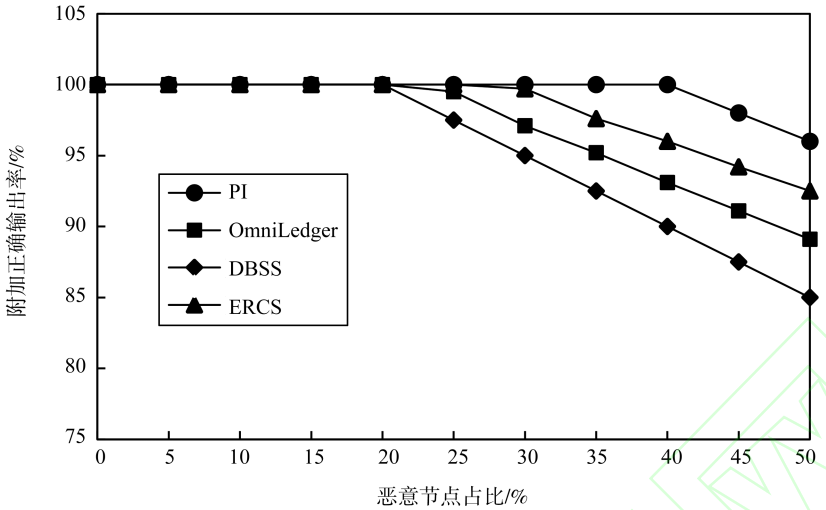

图 2　不同恶意节点占比下的附加正确输出率

Fig.2　Appended correct outputs under different malicious node proportion

3.3　吞吐量分析

在吞吐量方面,本文将 PI 算法的性能与 OmniLedger、DBSS 和 ERCS 三种算法进行了比较。为了与 PI 算法提出的分片模型相比较,其他 3 种算法的分片数量被调整为 $K=N/N_{\text{shmax}}$,以便每个分片由 N_{shmax} 个节点验证输出,其中 $N_{\text{shmax}}=\max\limits_{N_k\in\Pi} N_k$ 为式(24)中的最佳值。模拟了在固定恶意节点占比为 30%时,增加区块链节点总数 N 时所有算法的总吞吐量和平均块延迟。

从图 3 可以观察到,由于节点总数的不断增加,所有算法的平均吞吐量都在增加,但增长速率不同,在 DBSS、OmniLedger 和 ERCS 算法中增长率较低,而 PI 算法的增长率较高,基本上能保持线性增长,即单个分片的吞吐量基本保持不变。这是因为在 DBSS 算法和 OmniLedger 中,分片是分别基于 PoW 和随机抽样的结果形成的,而在基于可信度的区块链中,验证节点是根据的可信度选择的,因此在分片形成期间,节点的位置和对其分片中其他节点的看法被忽略,在大量节点时会导致越来越大的块延迟。图 4 中在节点总数不断增加时,所有算法的块延迟都会有所增加,但 PI 算法的增长率很低,这是因为在 PI 算法中,每个节点可以选择最大化节点收益的分片,这就取决于吞吐量和块延迟,越高的吞吐量和越低的块延迟才能使节点的收益最大化。通过系统总吞吐量和平均块延迟的比较,相比其他方案,PI 算法能够保证系统的单个分片的吞吐量和延迟基本保持不变。

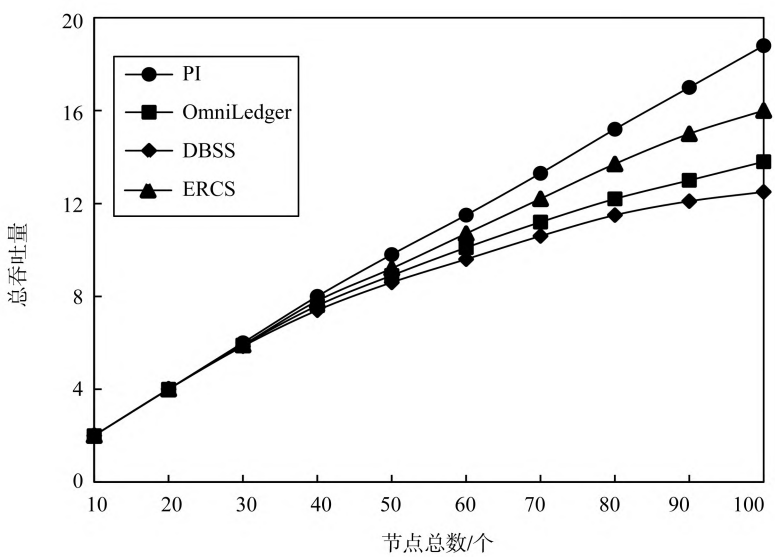

图 3　不同节点数下的总吞吐量

Fig.3　Total throughput under different number of nodes

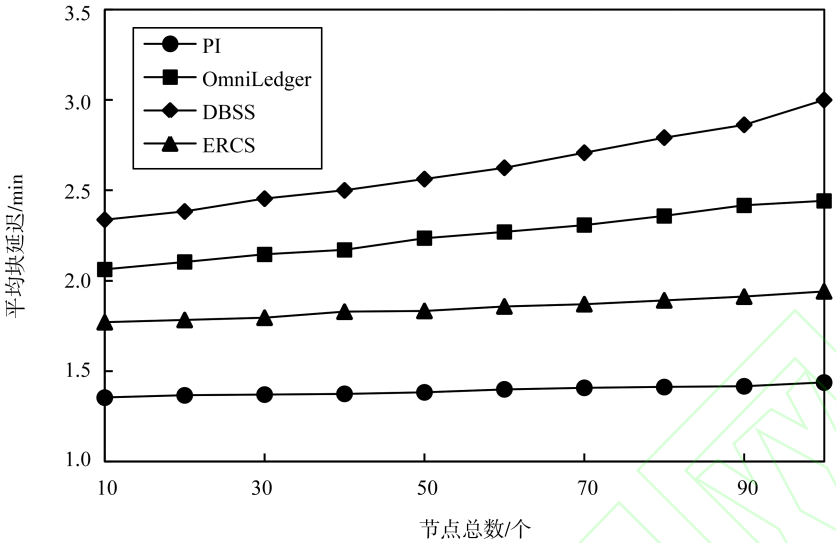

图 4 不同节点数下的平均块延迟

Fig.4 Average block delay under different number of nodes

4 结论

基于边缘计算的区块链系统对吞吐量和时延的要求较高,可以采用分片技术来提高区块链的可扩展性,但分片会降低区块链的稳定性,另外同一分片内的节点可能会因距离较远增加区块传播时间,降低系统吞吐量,因此需要一种分片方案能够在不降低吞吐量的同时提高区块链系统的稳定性。本文提出一种收益激励(PI)算法,首先针对单个节点计算其生成一个区块的延迟和能耗,计算出该节点处理任务的最终收益;其次根据基于边缘计算的可信度模型计算出该节点的平均分片可信度,在不降低其他节点收益和平均分片可信度的同时,该节点选择能够最大化其收益的分片;最后得到所有节点收益和分片可信度均最大化的分片结构。仿真结果表明,收益激励算法能够在保证吞吐量不降低的情况下,提高区块链的稳定性。区块链分片是一个非常有挑战性的方向,在研究了具有更高稳定性的分片方案后,将着手对区块链分片的共识协议进行研究,提高分片的共识效率。

参考文献:

[1] 武继刚,刘同来,李境一,等.移动边缘计算中的区块链技术研究进展[J].计算机工程,2020,46(8):1-13.
WU Jigang, LIU Tonglai, LI Jingyi, et al. Research progress on blockchain technology in mobile edge computing[J]. Computer Engineering, 2020, 46(8):1-13.

[2] 程冠杰,黄净杰,邓水光.基于区块链与边缘计算的物联网数据管理[J].物联网学报,2020,4(2):1-9.
CHENG Guanjie, HUANG Zhengjie, DENG Shuiguang. Data management based on blockchain and edge computing for Internet of Things[J]. Chinese Journal on Internet of Things, 2020, 4(2):1-9.

[3] 徐恪,凌思通,李琦,等.基于区块链的网络安全体系结构与关键技术研究进展[J].计算机学报,2021,44(1):55-83.
XU Ke, LING Sitong, LI Qi, et al. Research progress of network security architecture and key technologies based on blockchain[J]. Chinese Journal of Computers, 2021, 44(1):55-83.

[4] YOO H, YIM J, KIM S. The blockchain for domain based static sharding[C]//IEEE TrustCom 2018. New York:IEEE, 2018:1689-1692.

[5] KOKORIS-KOGIAS E, JOVANOVIC P, GASSER L, et al. OmniLedger:a secure, scale-out, decentralized ledger via sharding[C]//2018 IEEE Symposium on Security and Privacy (SP).San Francisco:IEEE, 2018:583-598.

[6] KANG J W, XIONG Z H, NIYATO D, et al. Toward secure blockchain-enabled Internet of vehicles:optimizing consensus management using reputation and contract theory[J]. IEEE Transactions on Vehicular Technology, 2019, 68(3):2906-2920.

[7] YUN J, GOH Y, CHUNG J M. DQN-based optimization framework for secure sharded blockchain systems[J]. IEEE Internet of Things Journal, 2021, 8(2):708-722.

[8] HUANG C Y, WANG Z Y, CHEN H X, et al. RepChain:a reputation-based secure, fast, and high incentive blockchain system via sharding[J]. IEEE Internet of Things Journal, 2021, 8(6):4291-4304.

[9] YANG Z, YANG K, LEI L, et al. Blockchain-based decentralized trust management in vehicular networks[J]. IEEE Internet of Things Journal, 2019, 6(2):1495-1505.

[10] 杨天,田霖,孙茜,等.移动边缘计算中基于用户体验的计算卸载方案[J]. 计算机工程,2020,46(10):33-40.
YANG Tian, TIAN Lin, SUN Qian, et al. Computing offloading scheme based on user experience in mobile edge computing [J]. Computer Engineering, 2020, 46(10):33-40.

[11] MASHAYEKHY L, GROSU D. A reputation-based mechanism for dynamic virtual organization formation in grids[C]//2012 41st International Conference on Parallel Processing. September 10-13, 2012, Pittsburgh, PA, USA. IEEE, 2012:108-117.

[12] 汪澍,许翀寰,汤中运. 基于信誉的二阶段溯源区块链共识策略[J]. 计算机工程,2021,47(7):109-116.
WANG Shu, XU Chonghuan, TANG Zhongyun.Reputation-based two-stage traceability blockchain consensus strategy[J]. Computer Engineering, 2021, 47(7):109-116.

[13] WANG W B, HOANG D T, HU P Z, et al. A survey on consensus mechanisms and mining strategy management in blockchain networks[J]. IEEE Access, 2019, 7:22328-22370.

[14] PÉREZ G O, ALBERTO HERNÁNDEZ J, LARRABEITI LÓPEZ D. Delay analysis of fronthaul traffic in 5G transport networks[C]//2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB). September 12-15, 2017, Salamanca, Spain. IEEE, 2018:1-5.

[15] DECKER C, WATTENHOFER R. Information propagation in the Bitcoin network[C]//IEEE P2P 2013 Proceedings. September 9-11, 2013, Trento, Italy. IEEE, 2013:1-10.

[16] ASHERALIEVA A, NIYATO D. Learning-based mobile edge computing resource management to support public blockchain networks[J]. IEEE Transactions on Mobile Computing, 2021, 20(3):1092-1109.

[17] 韩璇,袁勇,王飞跃.区块链安全问题:研究现状与展望[J].自动化学报,2019,45(1):206-225.
HAN Xuan, YUAN Yong, WANG Feiyue. Security problems on blockchain:the state of the art and future trends[J]. Acta Automatica Sinica, 2019, 45(1):206-225.

[18] WANG G. RepShard:reputation-based sharding scheme achieves linearly scaling efficiency and security simultaneously[C]//2020 IEEE International Conference on Blockchain (Blockchain). November 2-6, 2020, Rhodes, Greece. IEEE, 2020:237-246.

[19] HUANG X G, WANG Y S, CHEN Q B, et al. Security analyze with malicious nodes in sharding blockchain based fog computing networks[C]//2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall). September 27-30, 2021, Norman, OK, USA. IEEE, 2021:1-5.

[20] SETHI P, SARANGI S R. Internet of Things:architectures, protocols, and applications[J]. Journal of Electrical and Computer Engineering, 2017, 2017:1-25.

(编辑:祁业卿)