可信激励算法对区块链移动节点共识优化研究

刘 云，马 儀，田 地，李公瑾
(昆明理工大学信息工程与自动化学院，昆明 650500)

摘 要：节点可移动的物联网应用区块链时将节点称为区块链移动节点，区块链移动节点存在通信连通时间较短、算力和存储能力不足等问题导致网络达成共识时安全性和吞吐量较低. 本文提出一种可信激励算法对共识过程进行优化，首先区块链移动节点接收共识所需信息完成初始化；其次每个区块链移动节点生成决策块，决策块包含对验证消息的投票结果、自身的可信因子和决策块的生成时间，根据决策块在相邻区块链移动节点组成的集群中选出中继节点，中继节点传播验证消息到下一个集群，并产生区块存储在边缘服务器，一个中继为一跳，当跳数大于网络阈值跳数时完成共识；最后根据激励机制对节点奖励或惩罚，并按激励情况更新节点的行为标识反馈到共识. 仿真结果表明，与应用在同样网络情况的 PoET 和 PoS 算法相比，可信激励算法在保证了一定的吞吐量情况下，有效降低验证消息验证失败率提高了共识安全性，更适合节点可移动的物联网网络.

关键词：移动节点；决策块；可信因子；共识算法；吞吐量；安全性
中图分类号：TP393 **文献标识码**：A DOI：10.19907/j.0490-6756.2022.062004

Research on consensus optimization of trusted incentive algorithm forblockchain mobile nodes

LIU Yun, *MA Yi*, *TIAN Di*, *LI Gong-Jin*
(Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650500, China)

Abstract: When applying blockchain in the Internet of things with mobile nodes, these nodes are called blockchain mobile nodes. Blockchain mobile nodes have problems such as short communication connection time, insufficient computing power and storage capacity, resulting in low security and throughput when the network reaches a consensus. To tackle these drawbacks, a trusted incentive algorithm is proposed to optimize the consensus process. First the blockchain mobile node receives the information required by the consensus and completes the initialization. Secondly, each blockchain mobile node generates a decision block, which contains the voting result of the verification message, its own credibility factor and the generation time of the decision block. A relay node is selected from the cluster composed of adjacent blockchain mobile nodes by the decision block. The relay node propagates the verification message to the next cluster and the generated blocks are stored in the edge server. One relay is one hop, the consensus is completed when the number of hops is greater than the network threshold number of hops. Finally, the network rewards or punishes the nodes according to the incentive mechanism, and

收稿日期：2022-04-07
基金项目：国家自然科学基金(61761025)；云南省重大科技专项计划(202002AD080002)
作者简介：刘云(1973—)，男，云南昆明人，副教授，主要研究领域为物联网、区块链和数据挖掘等. E-mail：liuyun@kmust.edu.cn
通讯作者：马儀. E-mail：mayi7131@163.com

updates the behavior identifications of the nodes according to the incentive situation, the behavior identifications is then fed back to the consensus. The simulation results show that compared with the POET and POS algorithms applied in the same network, the trusted incentive algorithm can effectively reduce the verification failure rate of verification messages and improve the consensus security under the condition of ensuring a certain throughput. It is more suitable for the Internet of things with mobile nodes.

Keywords: Mobile node; Decision block; Reliability facto; Consensus algorithm; Throughput; Security

1　引　言

节点可移动的物联网结合区块链能保障网络中数据的安全性和可靠性,实现安全可信的通信[1],这类物联网节点称为区块链移动节点.网络结合区块链时存在两方面的问题:(1) 区块链移动节点间通信连通时间较短从而会产生通信传输速率的变化,造成通信失败或传输延迟[2];(2) 区块链移动节点本身的计算能力和存储能力有限,需使用边缘服务器辅助网络达成共识[3,4],但完全依赖边缘服务器达成共识是一个昂贵的解决方案[5-7].这些问题会影响网络达成共识的吞吐量[8]和网络安全性[9-11].

Salimitari 等[12]使用 PoET 共识算法来提高可移动节点区块链网络的交易吞吐量.PoET 算法中每个节点通过等待时间来获得创建区块的权利,等待时间遵循方案确定的概率分布,用户生成块的同时生成等待活动的 SGX 硬件协助证明与块一起提交.且算法采用统计测试来检查客户的等待时间来确定遵循何种概率分布,能减轻网络产生块所需要的算力并增加吞吐量.Nguye 等[13]基于 PoS 共识能耗低,时延小的特性;将其应用在移动节点的物联网中,通过评估持有的激励数量和时长,来决定节点获得记账权的几率,解决了网络中计算力不足,吞吐量不足的问题.

PoET 与 PoS 等共识算法提高了移动节点物联网网络吞吐量,但区块链移动节点网络中还存在移动性带来的安全性的问题[2].本文提出可信激励算法(Trusted Incentive Algorithm),对区块链移动节点网络的共识过程进行优化.首先,区块链移动节点以规定的信标频率传输自身的位置和速度给边缘服务器,并接收边缘服务器更新的共识所需的阈值票数,最大跳数,节点分布密度,节点行为标识等参数,以及上一个中继节点或消息发出者的验证消息完成初始化.其次每个区块链移动节点生成一个决策块,里面包含节点对验证消息的投票结果、根据概率预测信道质量好坏得到的自身可信因子,以及受可信因子和节点行为标识限制的决策块的生成时间;据决策块按照共识激励流程在相互靠近的区块链移动节点组成的集群中选出中继节点,中继节点产生区块并传播消息到下一个集群,产生的区块存储在边缘服务器上[14,15];每个中继节点作为传播验证消息的一跳,当跳数大于网络阈值跳数时证明消息传播到整个网络从而完成共识.最后根据投票结果判断节点好坏,按照激励机制奖励诚实节点、惩罚恶意节点;每一轮共识都按照激励结果对节点行为标识,使受到奖励的节点减少决策块生成时间,增加其成为中继节点的可能,加快共识进度.仿真结果表明,可信激励算法与 PoET 和 PoS 算法相比,安全性较高,且能保证吞吐量,更适用于存在移动节点的网络.

2　区块链移动节点共识激励模型

2.1　区块链移动节点模型

区块链移动节点模型如图 1 所示,a 为消息发出者,b 为普通挖掘节点,c 为决策块,d 为中继节点,a、b、c、d 本质都是区块链移动节点,e 为边缘服务器.

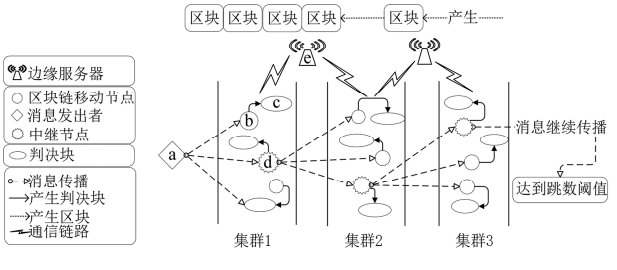

图 1　区块链移动节点模型

Fig. 1　Blockchain mobile node model

消息发出者发出验证消息,并为此支付一定的费用用于激励.边缘服务器接收普通挖掘节点按信标频率传播节点的位置和速度等信息,根据接收到的信息更新共识所需要的参数信息反馈给每一个节点,参数信息包括移动节点泊松分布密度参数 γ、节点的行为标识 P、选举中继节点时所需要的阈值票数 n_m 和网络阈值跳数 $n_{\max}$.其中,参数 $n_{\max}$ 和

n_m 的值可以由边缘服务器调节来适应网络条件与需求. 普通挖掘节点由每个注册加入区块链的物联网移动节点组成，相互靠近的普通挖掘节点组成集群，在集群中进行中继节点选择[16]，每个普通挖掘节点产生一个包含对验证消息的投票结果、可信因子 R 和决策块生成时间 τ 三个因素的决策块，根据决策块在集群中选出中继节点. 中继节点传播消息到下一个集群，产生区块存储在边缘服务器中. 每一个中继节点是一跳，定义跳数为 hop，当 hop 大于 $n_{\max}$，证明消息传播到整个网络，共识结束.

移动节点通过注册加入区块链网络，获取专属钱包地址和一对公钥私钥来进行隐私保护通信. 引入可信因子判决选出的中继节点具有最佳的信道质量，能在节点移动时更好地传播消息，且模型实现了一个节点一票的机制.

2.2　区块链移动节点共识激励流程

区块链移动节点共识激励过程如图 2 所示，普通挖掘节点接收消息完成初始化，再对验证消息投票判定消息为真或为假，并计算可信因子 R 和决策块生成时间 τ 来与集群里的节点比较.

选择信道质量好的节点作为中继来提高消息发送成功率，即可信因子 R 表示为发送方和接收方之间的信道质量，可信因子高表示信道质量较好. 定义距离因子 D 来表示的节点到发送方的距离大于在较长距离上成功传输的阈值的概率，定义 T 为概率预测节点收到消息到达成共识的时间总和；$T=t_1+\Delta t$，t_1 是事件消息从发送方到接收方接收到的时间，Δt 是达成共识的平均时间延迟. 以节点 i 为例，定义两个中继节点之间最小距离为 $d_{hop}^{\min}$，D_i^T 是在 T 时刻节点 i 和上一跳中继节点的距离大于 $d_{hop}^{\min}$ 的概率. R_i 表示为式(1). 表示为预测信号与干扰加噪声比($SINR$)[17]和距离因子 D 的乘积.

$$R_i=R(SINR_i^T)\cdot D_i^T \tag{1}$$

如式(2)决策块生成时间 τ_i 满足均匀分布，目的是为防止所有节点在同一时间传输消息，产生网络风暴，以及多个节点的 R 都是最大时，以 τ 较小的节点作为中继节点解决分叉问题. τ_i 的上限和下限为 a_i，b_i；a_i，b_i 受可信因子与激励制度下定义的节点行为标识的调控，能保证善良的、可信因子高的节点更有可能选为中继节点，加快网络达成共识.

$$\tau_i\sim\mu(a_i,b_i) \tag{2}$$

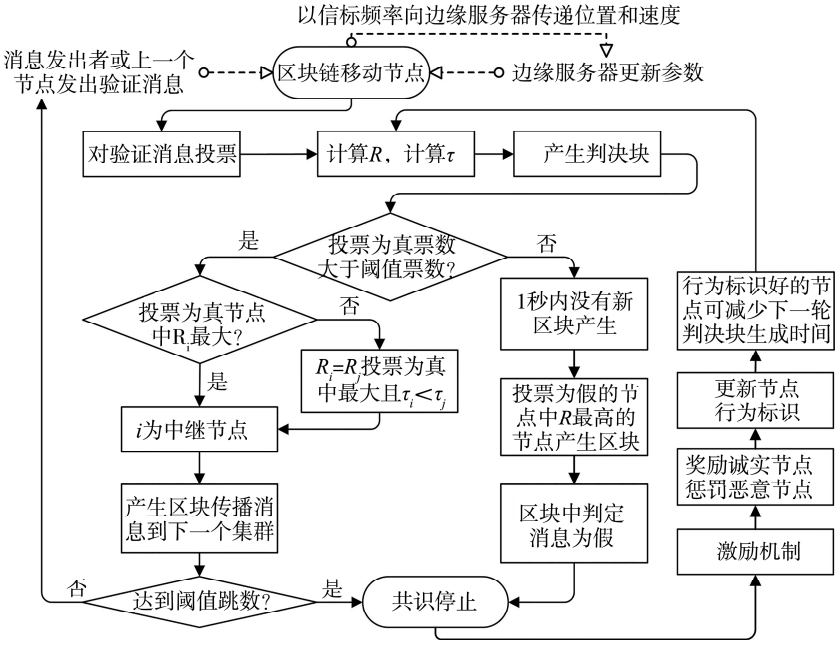

图 2　区块链移动节点共识流程

Fig. 2　Blockchain mobile node consensus process

如图 2，节点 i 将投票结果、R_i 和 τ_i 封装在产生的决策块中，当集群中投票为真票数达到阈值票数，R_i 在投票为真节点中最大，或 $R_j=R_i$ 同为最大但 $\tau_i<\tau_j$ 时，选节点 i 作为中继转发消息到下一个集群并产生区块存储在边缘服务器. 当跳数大于阈值跳数时共识停止. 如果某个集群中投票为真票数小于阈值票数，且集群在 1 秒内没有新区块产生，节点 i 的投票为假且在投票为假的节点中可信

因子最高,则由节点 i 产生一个区块判定消息为假. 共识提前终止. 共识结束后按照激励机制对节点进行激励或者惩罚,以此来更新节点的行为标识,下一轮共识时通过行为标识作用决策块生成时间来对共识正向反馈.

3　可信激励共识算法

该部分首先推导参数 R 与 τ,提出激励制度并给出激励制度中定义的节点行为标识对 τ 的作用关系. 参照图 2,结合共识和激励过程,给出可信激励共识算法.

3.1　可信因子推导

由 2.2 中式(1),区块链移动节点 i 的可信因子 R_i 定义为节点与集群中其余节点在 T 时刻的信号加干扰噪声比 $SINR_i^T$ 以及距离因子 D_i^T 之间的乘积.

预测区块链移动节点的 $SINR$ 依赖节点间的距离,而节点间的距离随时间的变化而变化,建立移动模型来预测 $SINR$,预测节点 i,j 之间 $SINR$ 的移动模型如式(3).

$$SINR_{i,j}=\frac{(d_{i,j})^{-\alpha}}{P_{\text{noise}}+\sum_{k=1,k\neq i}^{n_e}(d_{j,k})^{-\alpha}} \tag{3}$$

其中,位置或距离被视为随机变量,遵循某种概率分布[18]. α 为路径损耗指数[18],值取决于衰落环境;$d_{i,j}$ 为节点 i 与节点 j 的距离;$d_{j,k}$ 为节点 j 与干扰节点 k 的距离;n_e 为干扰节点数;P_{noise} 为噪声功率,仿真时给出.

对于成功的消息传输,在 T 时刻 $SINR$ 要超过一定的阈值 β,β 在仿真时给出,即在 T 时 $SINR_{i,j}^T\geqslant\beta$ 的概率如式(4)所示.

$$\begin{aligned}&Pr(SINR_{i,j}^T\geqslant\beta)=\\&Pr\left(\frac{(d_{i,j})^{-\alpha}}{P_{\text{noise}}+\sum_{k=1,k\neq i}^{n_e}(d_{j,k})^{-\alpha}}\geqslant\beta\right)=\\&Pr\left(d_{i,j}^T\leqslant\left(\beta\left(P_{\text{noise}}+\sum_{k=1,k\neq i}^{n_e}(d_{j,k})^{-\alpha}\right)\right)^{-\frac{1}{\alpha}}\right)\end{aligned} \tag{4}$$

其中,$d_{i,j}^T=d_{i,j}^{t_1}+\Delta d_{i,j}^{\Delta t}$ 是节点 i 和节点 j 在 T 时刻的距离,$\Delta d_{i,j}^{\Delta t}$ 是节点 i 和 j 在 Δt 期间的相对距离变化. $d_{i,j}^{t_1}$ 在节点与边缘服务器交换信息中,用标准高斯分布的概率密度函数(PDF)预测[18],一个节点的速度遵循标准的高斯分布,即节点 i 速度 $v_i\sim N(0,\sigma_i^2 t)$,其中的 $\sigma_i^2=[((v_i^{t_1}-v_i^{t_0})^2)/(t_1-t_0)]$ 是 v_i 的方差,t_0 与 t_1 的是节点 i 向边缘服务器传输速度与位置的时刻,$v_i^{t_0}$ 和 $v_i^{t_1}$ 表示为 v_i 在 t_0 与 t_1 时的速度. 据高斯变量的线性组合原理.

$$\Delta d_{i,j}^{\Delta t}=(v_i^{t_1}-v_j^{t_1}+\Delta v_i^{\Delta t}-\Delta v_j^{\Delta t})\Delta t \tag{5}$$

$$\Delta v_i^{\Delta t}\sim N(0,\sigma_i^2\Delta t) \tag{6}$$

$$\Delta v_i^{\Delta t}-\Delta v_i^{\Delta t}\sim N(0,(\sigma_i^2+\sigma_j^2)\Delta t) \tag{7}$$

其中 $\Delta v^{\Delta t}$ 是在 Δt 过程中的速度变化. 即 $\Delta d_{i,j}^{\Delta t}$ 如下式所示.

$$\Delta d_{i,j}^{\Delta t}\sim N(0,(\sigma_i^2+\sigma_j^2)\Delta t^3) \tag{8}$$

即 $\Delta d_{i,j}^{\Delta t}$ 是一个标准高斯变量. n_e 和 $d_{j,k}^T$ 对于节点 i 是未知的,所以通过估计期望值来找到 $\Pr(SINR_{i,j}^T\geqslant\beta)$,式(4)重写为 $Pr(SINR_{i,j}^T\geqslant\beta)=(\beta(P_{\text{noise}}+E(n_{\text{itf}})E(d_{j,k}^T)^{-\alpha})^{-(1/\alpha)}$,其中 $E(\cdot)$ 表示为期望值. 即对 $\Pr(SINR_{i,j}^T\geqslant\beta)$ 的计算转化为计算期望值.

假设移动节点的位置遵循独立齐次空间的泊松分布,密度参数为 γ nodes/km^2[1]. 使得节点可以动态移动. 节点的传输范围是一个半径为 r 的均匀圆形区域,即期望 $E(n_e)$ 可估计为节点 i 传输范围内其余的移动节点的数量. 其中的 γ 是预定义的,发布到每个节点.

$$E(n_e)=\sum_{k=1}^{\pi R^2\gamma}([((\pi r^2\gamma)^k)/(k!)]e^{-\pi r^2\gamma})-1 \tag{9}$$

面积为 πR^2 的圆形区域坐标(X,Y)处,干扰节点的正态分布概率密度函数定义为[[1/πr^2]][17]. 因此,$E(d_{j,k}^T)$ 表示为式(10).

$$E(d_{j,k}^T)=\int(X^2+Y^2)f(X,Y)\mathrm{d}X\mathrm{d}Y \tag{10}$$

将 $X=z\cos\varphi$ 和 $Y=z\sin\varphi$ 带入式(10)中,得到:

$$E(d_{j,k}^T)=\int_{d_{\text{neigh}}^{\min}}^{r}\int_0^{2\pi}\frac{z^2}{\pi r^2}\mathrm{d}\varphi\mathrm{d}z=\frac{2}{3r^2}(r^3-d_{\text{neigh}}^{\min\,3}) \tag{11}$$

结合式(4),令 $C=(\beta(P_{\text{noise}}+E(n_e)E(d_{j,k}^T)^{-\alpha})^{-(1/\alpha)}$. 以及 $d_{i,j}^T=d_{i,j}^{t_1}+\Delta d_{i,j}^{\Delta t}$,得到式(12).

$$\Delta d_{i,j}^{\Delta t}=\begin{cases}C+d_{i,j}^{t_1} & ①\\ C-d_{i,j}^{t_1} & ②\end{cases} \tag{12}$$

式(12)中,①式表示了节点 i 和节点 j 相互靠近;②式表示节点 i 和节点 j 相互远离. 即 $\Delta d_{i,j}^{\Delta t}$ 概率密度函数为

$$f(\Delta d_{i,j}^{\Delta t})=\frac{1}{\sqrt{2\pi(\sigma_i^2+\sigma_j^2)\Delta t^3}}e^{-\frac{(\Delta d_{i,j}^{\Delta t})^2}{2(\sigma_i^2+\sigma_j^2)\Delta t^3}} \tag{13}$$

累计概率密度函数定义如式(14).

$$F(\Delta d_{i,j}^{\Delta t})=\int_{-\Delta d_{i,j}^{\Delta t}}^{\Delta d_{i,j}^{\Delta t}}f(\Delta d_{i,j}^{\Delta t})d(\Delta d_{i,j}^{\Delta t}) \tag{14}$$

即当 $F(\Delta d_{i,j}^{\Delta t})=\Pr(d_{i,j}^T\leqslant C)=\Pr(SINR_{i,j}^T\geqslant\beta)$ 时 $\Pr(SINR_{i,j}^T\geqslant\beta)$ 的值如式(15).

$$\Pr(SINR_{i,j}^{T}\geqslant\beta)=\frac{1}{2}\left(erf\left(\frac{\Delta d_{i,j}^{\Delta t}}{\sqrt{2(\sigma_i^2+\sigma_j^2)}\,\Delta t^3}\right)-erf\left(\frac{-\Delta d_{i,j}^{\Delta t}}{\sqrt{2(\sigma_i^2+\sigma_j^2)}\,\Delta t^3}\right)\right) \tag{15}$$

同理，如果 $d_{i,j}^{t_1}>C$，因为 $d_{i,j}^{T}\leqslant d_x$，此时计算出 $\Pr(d_{i,j}^{T}\leqslant C)=\Pr(SINR_{i,j}^{T}\geqslant\beta)$ 的值如式(16).

$$\Pr(SINR_{i,j}^{T}\geqslant\beta)=1-\frac{1}{2}\left(erf\left(\frac{\Delta d_{i,j}^{\Delta t}}{\sqrt{2(\sigma_i^2+\sigma_j^2)}\,\Delta t^3}\right)-erf\left(\frac{-\Delta d_{i,j}^{\Delta t}}{\sqrt{2(\sigma_i^2+\sigma_j^2)}\,\Delta t^3}\right)\right) \tag{16}$$

$R(SINR_i^T)$ 为 $\Pr(SINR_{i,j}^{T}\geqslant\beta)$ 总和. 如式(17)所示，定义 n_{neigh} 是集群中除了节点 i 其余的邻居节点数目. 由式(15)(16)可知 $\Pr(SINR_{i,j}^{T}\geqslant\beta)<1$，则 $R(SINR_i^T)<n_{\text{neigh}}$，

$$R(SINR_i^T)=\sum_{j=1}^{j=n_{\text{neigh}}}\Pr(SINR_{i,j}^{T}\geqslant\beta) \tag{17}$$

由上面的推导可将 D_i^T 可转化为式(18)，结合式(15)和式(16). 得到 $D_i^T<1$.

$$D_i^T=\Pr(d_{i,k}^{t}>d_{\text{hop}}^{\min})=1-\Pr(d_{i,k}^{T}\leqslant d_{\text{hop}}^{\min}) \tag{18}$$

根据上面 R 的推导，据式(1)、式(17)和式(18)可以得到节点 i 的 R_i 范围为 $0<R_i<n_{\text{neigh}}$，R_i 越大的节点在集群中整体通信质量更高，更适合选择为中继节点.

3.2　激励反馈与决策块生成时间

为激励网络中节点合作，促进消息传递和数据共享，提高安全性，并对共识产生正向激励，提出一种奖励诚实挖掘节点、惩罚恶意挖掘节点的激励分配机制，引入决策块生成时间减少网络分叉，让集群中受到奖励的节点有更有可能成为中继节点.

3.2.1　*激励制度*　激励分配情况如表 1 所示，消息发出者支付一定的费用分成 A 和 B，对消息的真实性投票相反节点为恶意节点，假设 $hop=1$ 时网络中诚实节点个数 m，恶意节点个数为 n，$hop=1$ 处将 A 平均分配给集群中的诚实的挖掘节点上，B 在验证消息被验证为真时平均分配给网络的中继节点，如果最终消息被验证为假，则 B 当作发送伪消息的罚款给监管机构，a 是节点判断消息为假时节点所支付的费用. 目的是防止恶意虚假投票，促进真实消息的传播. 定义激励制度下节点行为标识 P. P 在每一轮共识结束后根据节点获得激励进行更新，行为标识为 1 的节点可减少决策块生成时间，使得其更有可能成为中继节点，节点能获得更多奖励，促进节点合作，加快网络完成共识.

$$P=\begin{cases}-1, & \text{当激励为}-a\text{ 时}\\ 0, & \text{当激励为 0 时}\\ 1, & \text{激励为其它时}\end{cases} \tag{19}$$

表 1　激励分配情况表

Tab. 1　Incentive distribution table

激励对象	行为	跳数	消息为真	消息为假
所有节点	诚实	$hop=1$	A/m	$(A/m)-a$
所有节点	恶意	$hop=1$	$-a$	0
中继节点	诚实	$hop=1$	$B/n_{\max}$	$m\cdot a$
中继节点	诚实	$hop<n_{\max}$	$B/n_{\max}$	0
中继节点	诚实	$hop=n_{\max}$	$n\cdot a$	0

3.2.2　*决策块生成时间*　以节点 i 决策块生产时间为例，由式(2)定义其满足均匀分布 $\tau_i\sim\mu(a_i,b_i)$，上下限受到激励制度下节点的行为标识 P 以及可信因子 R 调控，能更加可靠的选举中继节点且加速了共识过程. 其上下限 a_i 与 b_i 如式(20)所示，P_i 是节点 i 上一轮激励情况下节点的行为标识，表示 R 较高及激励制度中表现良好的节点的 τ_i 更短，由 3.1 节可知 $0<R_i<n_{\text{neigh}}$，其中 T_s 是成功传输投票的一个长度为 lBytes 的决策块的时间，如式(21)所示.

$$\begin{aligned}a_i&=\min(T_{\text{S}}^{1},T_{\text{S}}^{\text{all}})\cdot(n_{\text{neigh}}+1-R_i-P_i)\\ b_i&=\max(T_{\text{S}}^{1},T_{\text{S}}^{\text{all}})\cdot(n_{\text{neigh}}+1-R_i-P_i)\end{aligned} \tag{20}$$

$$T_S=\frac{l}{\delta_{\text{MAC}}}=\frac{T_a}{p_t\cdot p_s} \tag{21}$$

式(21)中 $p_t=2/(W+2)$ 为节点的平均传输概率，W 为 802.11 传输协议中分布式协调功能(DFC)的竞争窗口的大小，$p_s=n_t\cdot p_t\cdot(1-p_t)^{n_t-1}$，$\delta_{\text{MAC}}=P_t\cdot P_s\cdot(l/T_a)$，单位是(bit/s)，为节点设备中 MAC 层的吞吐量[19]，其中 n_t 是竞争同一信道的节点数量，当竞争窗口、数据包长度等变量固定时，T_S 才会随着 n_t 的变化而变化，T_S 当 $n_t=1$ 和 n_t 为所有挖掘节点时取两个边界值 T_{S}^{1} 和 T_{S}^{all}. T_a 为分布式协调函数(DCF)中一个时隙的平均长度.

3.3　可信激励算法

按照共识过程，参照图 2 移动节点共识流程图，可信激励共识算法如算法 1.

算法 1　可信因子共识算法

输入：阈值票数 n_m，最大跳数 $n_{\max}$，密度参数 γ，激励反馈 P

输出：区块

1) 集群中每个节点进行如下过程,以节点 i 为例;
2) Begin
3)　While($hop<n_{\max}$)//跳数小于阈值跳数
4)　　计算自身可信因子 R;
5)　　计算 $Pr(SINR_{i,j}^{T}\geqslant\beta)$;
6)　　$R(SINR_i^T)=\sum_{j=1}^{j=n_{\text{neigh}}}\Pr(SINR_{i,j}^{T}\geqslant\beta)$;
7)　　$D_i^T=\Pr(d_{i,k}^{t}>d_{hop}^{\min})$;
8)　　$R_i=R(SINR_i^T)\cdot D_i^T$;
9)　　产生决策块,计算决策块时间;
10)　　$\tau_i\sim\mu(a_i,b_i)$;
11)　　$a_i=\min(T_S^1,T_S^{\text{all}})\cdot(n_{\text{neigh}}+1-R_i-P_i)$;
12)　　$b_i=\min(T_S^1,T_S^{\text{all}})\cdot(n_{\text{neigh}}-R_i+1-P_i)$;
13)　　节点对验证消息投票为真或假;
14)　　if i 投票为真 && 投票为真票数 $>n_m$ && R_i 在集群中最大;
15)　　i 为中继节点,传播消息,产生区块;
16)　　else if $R_i=R_j$ && R_i,R_j 在集群中最大;
17)　　if $\tau_i>\tau_j$ && i 投票为真 && 投票为真票数 $>n_m$
18)　　选择 i 为中继节点,传播消息,产生区块;
19)　　end
20)　else 1 秒内投票为真票数 $<n_m$ && 投票为假的节点中 R_i 最大 && 节点 i 投票为假;
21)　　由节点 i 产生一个区块判定消息为假;
22)　　break;//跳出 Whlie 循环;
23)　　$hop=hop+1$;
24) End while;
25) 按照激励制度惩罚或奖励节点,并按照激励情况更新 P;
26) End

算法 1 表示区块链移动节点输入 n_m、$n_{\max}$、γ、P 等参数完成初始化后,在区块链移动节点组成的集群选出中继节点,输出产生的区块.

跳数 $hop<n_{\max}$ 进入循环,集群中每个普通挖掘节点计算的自身的可信因子、决策块生成时间并对验证消息投票.循环过程中用条件控制在集群中选择中继节点,以节点 i 为例,当满足 i 投票为真且投票为真票数达到阈值票数,以及集群中 R_i 最大的条件时,选择 i 为中继节点.当出现 i,j 投票为真,$R_i=R_j$ 同为集群中最大,且投票为真票数达到阈值票数的条件,选择 τ 比较小的节点为中继节点.投票为真票数小于阈值票数则判定消息为假并结束循环.中继节点传播消息到下一个集群,产生的区块作为循环单次输出;每个中继节点作为传播消息的一跳,当跳数大于网络阈值跳数时循环结束.并根据节点行为进行激励,更新节点行为标识 P.可信因子共识算法结束.

3.4　可信激励算法性能参数分析

为评估可信激励算法对于区块链移动节点网络共识的优化性能,对区块链移动节点网络评估其安全性与吞吐量两个重要参数,下面针对区块链移动节点网络安全性与吞吐量进行理论分析.

3.4.1　安全性　安全性定义为不改变交易的原始有效性状态的情况下,网络可以控制的恶意节点的数量,可控制的恶意节点数量越多,证明数据验证更可靠.以验证消息的失败率代表安全性,失败率越低代表安全性越高,假设节点发出假消息的概率为 P_f,验证失败记为 F,分为真消息验证失败 F_t 和假消息验证失败 F_f.

$$F=P_fF_t+(1-P_f)F_f \tag{22}$$

其中,F_f 为恶意节点满足成为中继节点的条件且接收到阈值的投票时,通过恶意投票将原来的假消息标记为真.F_t 为诚实节点没有收到投票为真的阈值票数来验证真实消息.据切尔洛夫界限[20]得到 F 的上下限 F_U、F_L 如下.μ_x 为诚实节点平均数量,h 为集群中恶意节点或诚实节点数量.

$$F_U=1-p_f+{p_f}^2\Pr(m\geqslant n_{\text{all}})_U-(1-p_f)^2\Pr(n\geqslant n_{\text{all}})_L \tag{23}$$

$$F_L=1-p_f+{p_f}^2\Pr(m\geqslant n_{\text{all}})_L-(1-p_f)^2\Pr(n\geqslant n_{\text{all}})_U \tag{24}$$

$$\Pr(h\geqslant n_m)_U=\begin{cases}e^{-[((n_{\text{all}}-\mu_x)^2)/(\mu_x+n_{\text{all}})]}, & n_m\geqslant\mu_x\\ 1, & \text{其他情况}\end{cases} \tag{25}$$

$$\Pr(h\geqslant n_m)_L=\begin{cases}1-e^{-[((\mu_x-n_{\text{all}})^2)/(2\mu_x)]}, & 0\leqslant n_m\leqslant\mu_x\\ 0, & \text{其余情况}\end{cases} \tag{26}$$

3.4.2 吞吐量　吞吐量定义为每秒生成的块的数量.本文中假设一个集群普通挖掘节点个数为 n_{all},则生成区块总的时长 T_g 的范围为

$$\min(T_S^1,T_S^{\text{all}})\cdot n_{\text{all}}\leqslant T_g\leqslant n_{\text{all}}\cdot\max(T_S^1,T_S^{\text{all}}) \tag{27}$$

定义 T_c 为加密密钥块所需要的时间.则按每秒生成的键块数量计算的吞吐量可以估计如式(28)所示.

$$\text{TPS}=\frac{1}{T_g+T_c} \tag{28}$$

4　仿真分析

4.1　仿真环境

软件使用 OMNeT++网络仿真软件结合进行城市流动性模拟(SUMO)来构造移动节点的环境进行仿真，仿真环境为 Win10，64 位操作系统，4.5 GHz CPU，16 G 内存的 PC. 仿真的参数如表 2 所示.

表 2　仿真参数表

Tab. 2　Simulation parameter table

参数	值	参数	值
通信协议	802.11 b	$d_{hop}^{\min}$	100 m
节点速度	0.60 m/s	α	3
仿真时间	200 s	P_{noise}	−99 dB
仿真区域	10 km×10 km	β	8 dB
信标频率	0.1 s	W	32
ι	756 Bytes	r	250 m
γ	100，130 或 175 nodes/km^2		

参数表明仿真的区域是 10 km×10 km 面积区域，区块链移动节点的速度在 0.60 m/s，两个中继节点之间的最短距离为 100 m，节点传输的范围为 250 m，决策块 l 大小为 756 Bytes，节点向边缘服务器传播位置、速度的信标频率为 0.1 s，802.11 协议中分布式协调功能(DFC)的竞争窗口 W 的大小设置为 32. 在相同的节点条件下对比使用 PoS 与 PoET 共识算法的网络的安全性与吞吐量.

4.2　安全性仿真分析与对比

如图 3 所示，为分析可信激励算法在集群节点数量与 p_f 不同时网络的验证失败率，p_f 设置为 0.3 与 0.7，普通挖掘节点数量设置为 10 到 40. n_m 设置为 3，即阈值票数小于平均诚实节点数. p_f 小的网络 F 更低，具有更高的安全性. 当诚实节点占多数时. p_f 较小的验证失败率 F 更低.

如图 4 所示，为比较可信激励算法，PoET 和 PoS 算法在 p_f、普通挖掘节点数量不同情况下的安全性. 将 p_f 设置为 0.1 到 0.9；普通挖掘节点数量设置为 15 和 25；n_m 固定在诚实节点平均数. 验证失败率越低表示安全性越高. 可信激励算法的消息验证失败率 F 低于 PoET 和 PoS，有更高的安全性. 因为 PoET 每个节点生成一个 0～1 s 之间的随机数来确定其收集微块的等待时间，等待时间不受边缘服务器的控制，可信激励算法由于共识机制原理在低 p_f 时和 PoET 的 F 接近；但 p_f 较高时，可信激励算法中 R 最高的诚实节点在 PoET 随机等待时间内的投票无法达到阈值票数，达成共识的时间会变长，因此 PoET 的 F 上升速度高于可信激励算法. 基于信誉的 PoS 算法中，一个节点的信誉超过一定的阈值则认为节点是诚实的. 在 0～100 的范围内随机分配一个声誉值给节点，因此声誉低于 50 的概率被定义为恶意节点. 使得恶意中继节点只转发来自恶意发送方的消息，而诚实中继节点只转发来自诚实发送方的消息. 其安全性也低于可信激励算法.

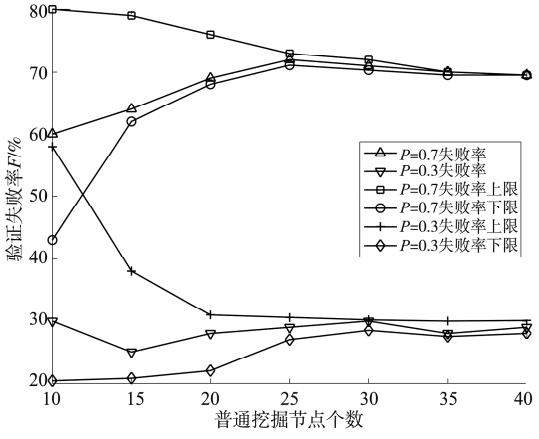

图 3　可信激励算法验证失败率图

Fig. 3　Graph of verification failure rate of Trusted incentive algorithm

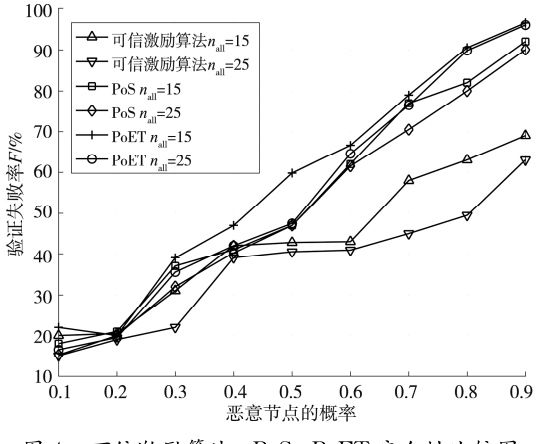

图 4　可信激励算法，PoS，PoET 安全性比较图

Fig. 4　Security comparison graph of trusted incentive algorithm，POS，PoET

可得出在区块链移动节点网络中使用可信激励算法优化共识得到的验证失败概率更低，安全性较高.

4.3　吞吐量仿真分析与对比

如图 5 所示，为分析可信激励算法在 p_f、普通挖掘节点数量不同情况下的吞吐量，将 p_f 设置为 0.1～0.9，n_{all} 设置为 15，25 和 35，n_m 固定在诚实

节点平均数. 可信激励算法的吞吐量随 n_{all} 和 p_f 的增加而逐渐减少. 在 $p_f=0.1$, $n_{all}=15$ 最高时 TPS 达到 11 block/s, 当 $p_f \geqslant 0.8$, $n_{all}=35$ 时最低是 0.9 block/s, 这意味着如果一个集群里有更多的挖掘节点, 可能无法达到生成块的最大允许延迟在 1 秒以内. 表明提出的算法在 p_f 和 n_{all} 值较低时表现出更好的性能.

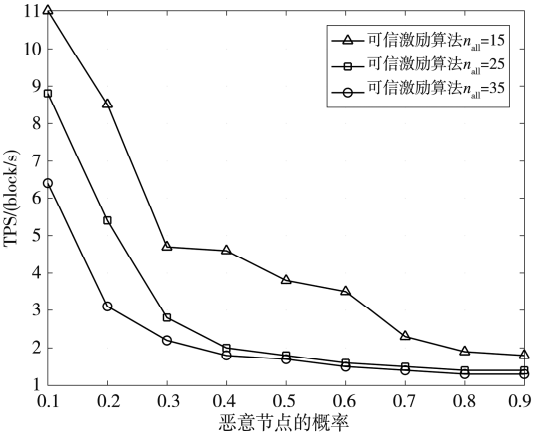

图 5　可信激励算法吞吐量图

Fig. 5　Throughput graph of trusted incentive algorithm

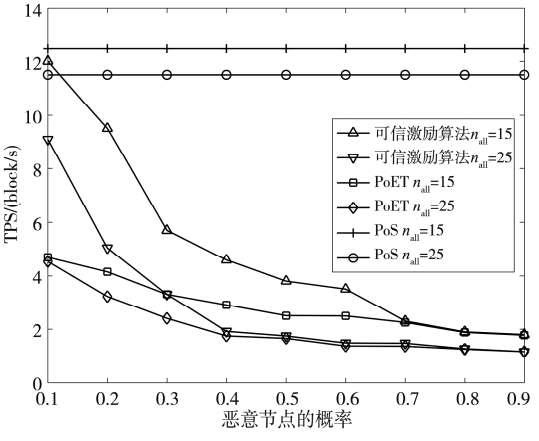

图 6　可信激励算法, PoET, PoS 吞吐量比较图

Fig. 6　Comparison graph of throughput of trusted incentive algorithm, PoET and POS

如图 6 所示, 为比较可信激励算法、PoET 和 PoS 算法在 p_f, 普通挖掘节点数量不同情况下的吞吐量. 将 p_f 设置为 0.1 到 0.9, 普通挖掘节点数量设置为 15 和 25, n_m 固定在诚实节点平均数. 可信激励算法的吞吐量介于 PoET 和 PoS 之间. 可信激励算法平均时延小于 PoET. 仿真也表明 p_f 较小的时候可信激励算法吞吐量优于 PoET; 但当 p_f 较大时, 可信激励算法接收到阈值诚信投票的等待时间更长, 这是因为恶意微块的生成频率增加, 造成与 PoET 之间的时延差变小. 由于 PoS 的时延与 p_f 无关, 只随着 n_{all} 的增加而增加. 基于信誉的消息验证方式消除了投票时间, 只消耗中继节点选择的时间, 所以基于 PoS 的吞吐量是三者之间最高的.

据上述分析, 可信激励算法为保障安全性, 采用投票验证方式牺牲了一定的吞吐量, 吞吐量高于 PoET 和略低于 PoS. 但可信激励算法安全性高于 PoET 和 PoS 共识算法, 其整体性能是最优的.

5　结　论

物联网节点可移动网络在结合区块链达成共识时存在通信失败或传输延迟等问题, 降低了网络的安全性和吞吐量. 文章提出一种可信激励算法对区块链移动网络共识进行优化, 首先引入决策块, 区块链移动节点通过生成含投票结果和可信因子的决策块, 并计算决策块生成时间. 通过决策块在相邻的区块链移动节点组成的集群选出中继节点来传播验证信息并产生区块, 以此逐步将验证信息传播到整个网络达成共识, 最后按激励制度对节点共识过程中的行为进行激励, 并以激励情况定义节点行为标识促进共识的完成. 通过仿真与 PoET 和 PoS 算法相比, 可信因子共识算法保证了一定的吞吐量情况下降低了验证失败率从而提高了安全性, 更适合有移动节点的网络. 在未来的工作中, 可用其它方式取代投票机制, 减少区块产生时间, 改善吞吐量, 使该共识算法在不同数量挖掘节点下都能有更好的性能.

参考文献:

[1] Kim S. Impacts of mobility on performance of blockchain in VANET [J]. IEEE Access, 2019, 7: 68646.

[2] Ayaz F, Sheng Z G, Tian D, *et al*. A Proof-of-Quality-Factor (PoQF)-based blockchain and edge computing for vehicular message dissemination [J]. IEEE Internet Things J, 2021, 8: 2468.

[3] Xu L, Ge M, Wu W. Edge server deployment scheme of blockchain in IoVs [J]. IEEE T Reliab, 2022, 71: 500.

[4] Shen S, Han Y, Wang X, *et al*. Computation offloading with multiple agents in edge-computing-supported IoT [J]. ACM Trans Sens Netw, 2019, 16: 1.

[5] Wagner M, McMillin B. Cyber-physical transactions: a method for securing VANETs with blockchains [C]//Proceedings of the 2018 IEEE 23rd Pa-

cific Rim International Symposium on Dependable Computing (PRDC). [S. l.]: IEEE, 2018.

[6] 刘云，宋凯，陈路遥，等. 最小损失算法在区块链物联网中的优化研究[J]. 四川大学学报：自然科学版，2022，59：023002.

[7] 雷鸣，崔晓丹，杨天舒，等. 区块链技术在智能电网稳定控制系统中的应用[J]. 江苏大学学报：自然科学版，2021，42：569.

[8] 刘云，朱鹏俊，陈路遥，等. 联合分布算法对区块链分片的稳定性分析优化研究[J]. 四川大学学报：自然科学版，2022，59：032001.

[9] 周畅，陆慧梅，向勇，等. 区块链在车载自组网中的应用研究及展望[J]. 计算机科学，2020，47：213.

[10] 王壹铭，初剑峰，王永军，等. 基于有向无环图的高效区块链共识算法[J]. 吉林大学学报：理学版，2020，58：1167.

[11] 曹傧，林亮，李云，等. 区块链研究综述[J]. 重庆邮电大学学报：自然科学版，2020，32：1.

[12] Salimitari M, Joneidi M, Fallah Y P. BATS: a blockchain-based authentication and trust management system in vehicular networks[C]//Proceedings of the 2021 IEEE International Conference on Blockchain, [S. l.]: IEEE, 2021: 333.

[13] Nguyen C T, Hoang D T, Nguyen D N, *et al*. Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities [J]. IEEE Access, 2019, 7: 85727.

[14] 张开元，桂小林，任德旺，等. 移动边缘网络中计算迁移与内容缓存研究综述[J]. 软件学报，2019，30：2491.

[15] 刘雷，陈晨，冯杰，等. 车载边缘计算中任务卸载和服务缓存的联合智能优化[J]. 通信学报，2021，42：18.

[16] Wang W, Hoang D T, Hu P Z, *et al*. A survey on consensus mechanisms and mining strategy management in blockchain network [J]. IEEE Access, 2019, 7: 22328.

[17] Sun Y, Zhang L, Feng G, *et al*. Blockchain-enabled wireless Internet of Things: performance analysis and optimal communication node deployment [J]. IEEE Internet Things J, 2019, 6: 5791.

[18] N Li, J-F, Díaz V H, *et al*. Probability prediction-based reliable and efficient opportunistic routing algorithm for VANETs [J]. IEEE/ACM Trans Netw, 2018, 26: 1933.

[19] Tian D, Zhou J, Chen M, *et al*. Cooperative content transmission for vehicular ad hoc networks using robust optimization [C]//Proceedings of the IEEE INFOCOM 2018- IEEE Conference on Computer Communications, Honolulu. [S. l.]: IEEE, 2018: 90.

[20] Wang J, Ding Y, Xiong N N, *et al*. GSCS: General secure consensus scheme for decentralized blockchain systems [J]. IEEE Access, 2020, 8: 125826.

引用本文格式：

中　文：刘云，马儀，田地，等. 可信激励算法对区块链移动节点共识优化研究[J]. 四川大学学报：自然科学版，2022，59：062004.

英　文：Liu Y, Ma Y, Tian D, *et al*. Research on consensus optimization of trusted incentive algorithm for blockchain mobile nodes [J]. J Sichuan Univ: Nat Sci Ed, 2022, 59: 062004.