物联网区块链中基于演化博弈的分片算法

徐小琼，孙 罡*，罗 龙

(电子科技大学光纤传感与通信教育部重点实验室 成都 611731)

【摘要】分片技术被广泛认为是一种克服当前物联网区块链系统可扩展性限制的有效解决方案。然而，由于恶意节点随机分布以及区块链网络复杂的参数配置，如何保证分片的有效性仍具有挑战。首先，对分片区块链的性能进行建模，分析其安全性和可扩展性。其次，为减少恶意节点的聚集以及提高网络的性能，提出了一种基于演化博弈的分片选择算法来优化节点的分片决策。仿真结果表明，提出的分片算法可以使恶意节点尽可能地均匀分布于各个分片中，同时提高分片区块链的性能，进而更好地支持区块链在物联网中的应用。

关 键 词 区块链； 演化博弈； 物联网； 分片算法

中图分类号 TN915 **文献标志码** A doi:10.12178/1001-0548.2022029

Sharding Algorithm Based on Evolutionary Game in the IoT-Blockchain

XU Xiaoqiong, SUN Gang*, and LUO Long

(Key Lab of Optical Fiber Sensing and Communications, University of Electronic Science and Technology of China Chengdu 611731)

Abstract To overcome the scalability limitations of the current internet of things (IoT) blockchain system, sharding technology is widely regarded as a promising solution. However, due to the random distribution of malicious nodes and the complex network configurable parameters, the effectiveness of sharding is still a challenging. This paper proposes the performance model to analyze the security and scalability of the sharding-based blockchain. Secondly, to reduce the gathering possibility of malicious nodes and improve the performance, this paper proposes a sharding selection algorithm based on the evolutionary game. The simulation results show that proposed algorithm can make the malicious nodes uniformly distributed in each shard and has better performance, thereby well supporting the applications in IoT-blockchain.

Key words blockchain; evolutionary game; IoT; sharding algorithm

物联网在传统互联网的基础上，通过传感器网络赋予物体互联互通的能力，因此极大程度地降低了日常生产和运营的成本[1]。但随着物联网设备的急剧增长和服务的广泛部署，其网络性能受到边缘终端设备以及云服务器传输宽带的制约，使得物联网传输速率劣化，带来了一定的安全隐患[2]。同时，对数据进行中心化管理使得物联网设备隐私安全性得不到保障。因此，物联网系统不可避免地存在诸如用户隐私泄露、DDoS 攻击等安全性的问题[3]。

区块链的出现为物联网下实现安全、高效的数据交互和隐私保护提供了新的解决方案[4]。区块链是一个新型的分布式数据账本，其可以对不断增长的物联网数据进行记录和维护以防止伪造和非法篡改。区块链通过密码学技术对数据进行加密，并将数据以区块的形式进行存储且将相关联的数据区块进行链状串联。这种链状的结构能利用 Merkle Tree 对数据进行校验，从而判断区块内的数据是否被篡改[5]。但由于现有的区块链架构存在可扩展性低、交易时延高的性能缺陷，仍不能很好地支撑物联网业务[6]。

为了满足区块链在物联网场景下的应用需求，近年来，已有一系列的区块链性能优化方案被提出。其中，网络分片被认为是解决区块链可扩展性问题及提升区块链性能最主要的技术之一[7-10]。分

收稿日期：2022－01－19；修回日期：2022－03－04
基金项目：国家自然科学基金 (62102066)
作者简介：徐小琼 (1992－)，女，博士生，主要从事区块链、云计算方面的研究.
*通信作者：孙罡，Email：gangsun@uestc.edu.cn

片通过将整个区块链网络拆分为多个子网络，每个子网络由一个不同的节点集合进行维护，交易在不同的子网络内并行处理。由于每个区块链节点不必处理系统中所有的交易，因此极大地提升了网络的交易处理性能。尽管如此，现有的区块链分片算法仍存在一些挑战[8]。首先，网络分片大小是需要考虑的问题，当网络分片数目较多，即每个分片内节点较少时，会导致共识的安全性问题。相反，当网络分片数目较少，则可并行的交易处理能力不够，网络性能无法满足应用需求。因此，在实际应用中，如何选择分片大小以平衡安全性和网络性能需求是需要解决的问题。其次，在基于实际拜占庭容错 (practical byzantine fault tolerance, PBFT) 共识算法的区块链网络中[11]，恶意节点的随机分布会导致某个分片内的恶意节点数目大于分片中所有节点的三分之一，这会出现个别分片无法对交易达成共识，进而产生分片失效的问题。因此，如何使恶意节点尽可能均匀地分布在不同的分片内以满足分片有效性是需要解决的又一问题。

针对这些问题，本文提出分片区块链安全性和可扩展性的理论分析模型。其次，基于提出的分析模型建立优化求解问题来解决可扩展性和安全性均衡问题。最后，基于演化博弈论得到较优的区块链分片算法使恶意节点尽可能地均匀分布于每个分片中。仿真结果表明，本文算法可以使不同类型节点的分布动态演化收敛到接近最优的均衡点，达到节点均匀分布的目的，进而在支持物联网应用的区块链中获得更好的性能。

1 相关工作

近年来，研究者们将分片技术应用到区块链中，使其成为解决区块链可扩展性问题的重要方案。区块链网络分片的关键思想是将网络划分成多个子集，称为分片，每个分片包含一部分区块链网络节点。所有的分片并行处理网络中不同的交易集，而不是整个网络节点处理相同的交易。由于每个分片内节点单独进行交易共识，节点只需要和同分片内的其他节点进行通信，因此大大降低了计算和通信的开销。迄今为止，已有大量的区块链分片协议被提出[12-15]。

文献 [12] 提出了一种可用于公有区块链的分布式分片算法 Elastico，其使用工作量证明 (power of work, PoW) 将网络矿工节点随机分配到较小的分片中，每个分片处理一组不相交的交易。然后，分片内部节点采用经典的 PBFT 共识算法并行处理交易。虽然 Elastico 能实现在拜占庭环境下的高可扩展性，但 Elastico 算法的分片选择不具有很强的偏差抗性。文献 [13] 在 Elastico 算法的基础上提出了一种新的分片算法 OmniLedger，该算法利用抗偏置随机协议 RandHound 和可验证随机函数来自主执行节点分片以确保分片的安全性。但在 OmniLedger 算法中，由于每个分片在进行几轮共识后就会被拆散重构，分片重构太过频繁带来较高的分片切换时延。

文献 [14] 采用可信执行环境 (trusted execution environment, TEE) 设计了一个高效安全的分片生成协议，其在分布式设置中实现了一个可信的随机信标来生成无偏随机值，同时利用 TEE 来增加拜占庭共识算法的容错能力以减少分片大小。文献 [15] 提出了公有区块链的分片算法 RapidChain，其可以使整个网络容忍高达 33% 的恶意节点或故障节点，每个分片内可以容忍近 50% 的恶意节点。同时，在没有任何可信假设的情况下，RapidChain 算法能实现通信、计算和存储的完全分片，具有更高的吞吐量。

尽管上述的分片算法在一定程度上实现了区块链的高可扩展性，但随着网络恶意节点数量的增加，如何获得一个较优的分片算法，使得恶意节点均匀分布在每个分片以降低分片失效概率，是一个亟待解决的问题。

2 分片性能分析

本节首先对分片区块链的安全性和可扩展性进行理论分析。基于分析模型，本节建立分片优化求解问题来实现分片区块链安全性和可扩展性的均衡。

2.1 分析模型

在基于 PBFT 共识算法的区块链网络中，安全性和可扩展性指标的相关定义为：

1) 安全性：分片区块链的安全性可以由分片内交易失效概率来衡量，被定义为分片中恶意节点数目超过能容忍最大恶意节点的界限。分片交易的失效概率越低，则代表网络安全性越高。

2) 可扩展性：分片区块链的可扩展性一般由分片后交易吞吐量和交易平均时延来衡量。交易吞吐量被定义为网络中平均每秒执行的交易数目，交易平均时延被定义为交易从提交到上链整个过程花费的平均时间。交易吞吐量越高，交易平均时延越低，网络可扩展性越高。本文仅考虑交易共识阶段

的可扩展性，即交易共识吞吐量和交易共识时延。

2.1.1　失效概率分析模型

在分片区块链中，如何指派网络节点到不同的分片问题可以转化为不放回抽样问题。因此，本文采用超几何分布来计算分片后交易的失效概率[16]。

假设网络中总的节点数目为N，恶意节点数目为M，网络中分片的数目为N_{s}，每个分片具有相等的分片大小，因此分片内的节点数目为$n=N/N_{\mathrm{s}}$。令随机变量X表示分片中恶意节点的数量，$P(X=k)$表示包含n个节点的分片中存在k个恶意节点的概率：

$$P(X=k)=\frac{C_M^k C_{N-M}^{n-k}}{C_N^n} \tag{1}$$

其均值为：

$$E(X)=(nM)/N \tag{2}$$

方差为：

$$\mathrm{Var}(X)=\frac{nM}{N}\left(1-\frac{M}{N}\right)\left(1-\frac{n-1}{N-1}\right) \tag{3}$$

在基于 PBFT 共识的区块链中，分片内能容忍的最大恶意节点数为$N_{\mathrm{m}}=(n-1)/3$。因此，分片后交易失效概率P_f可以表示为：

$$P_f=P(X\geqslant N_{\mathrm{m}})=\sum_{k=N_{\mathrm{m}}}^{n}\frac{C_M^k C_{N-M}^{n-k}}{C_N^n} \tag{4}$$

在分片区块链中，如果某个分片内恶意节点数目过多，分片内节点无法对交易达成共识。为了避免分片交易失效对整个性能的影响，本文定义了一个安全参数λ来限制分片失效概率，如果满足以下不等式，则分片是足够安全的：

$$P_f\leqslant 2^{-\lambda} \tag{5}$$

利用切比雪夫界[17]可知，对于任意的$a\geqslant 0$有：

$$P(|X-E(X)|\geqslant a)\leqslant\frac{\mathrm{Var}(X)}{a^2} \tag{6}$$

因此，分片交易失效概率P_f的上界可以表示为：

$$P_f=P(X\geqslant N_{\mathrm{m}})=$$
$$P(|X-E(X)|\geqslant(N_{\mathrm{m}}-E(X)))\leqslant\frac{\mathrm{Var}(X)}{(N_{\mathrm{m}}-E(X))^2} \tag{7}$$

联合式 (5) 和 (7) 有：

$$\frac{\mathrm{Var}(X)}{(N_{\mathrm{m}}-E(X))^2}<2^{-\lambda} \tag{8}$$

2.1.2　网络交易吞吐量分析模型

区块链中，网络交易吞吐量直接取决于两个参数：每个区块包含的交易数目，即区块大小S^{B}字节以及区块成块间隔T_{I}。假设分片后每个分片内包含的恶意节点数目未超过分片内总节点数目的三分之一，即满足 PBFT 共识算法的要求，则区块链总交易吞吐量为各个分片的交易吞吐量之和。总交易吞吐量TH为：

$$\mathrm{TH}=\sum_{i=1}^{N_{\mathrm{s}}}\mathrm{TH}_i \tag{9}$$

假设区块的头部大小为$S_{\mathrm{H}}^{\mathrm{B}}$字节，区块内每笔交易的平均大小为$\beta$(字节)，则每个分片的交易处理速率为$(S^{\mathrm{B}}-S_{\mathrm{H}}^{\mathrm{B}})/\beta/T_{\mathrm{I}}$，于是有：

$$\mathrm{TH}=\sum_{i=1}^{N_{\mathrm{s}}}\left\lfloor(S^{\mathrm{B}}-S_{\mathrm{H}}^{\mathrm{B}})/\beta\right\rfloor/T_{\mathrm{I}} \tag{10}$$

2.1.3　交易平均时延分析模型

PBFT 的共识算法包含 3 个阶段：pre-prepare 阶段、prepare 阶段以及 commit 阶段。主节点接收到来自客户端的交易请求后，发送一个共识消息到其他节点。节点执行 PBFT 的 3 阶段共识流程，返回消息到客户端，客户端收到来自$f+1$个节点的相同消息之后完成共识[18]。根据文献 [19] 可知，分片交易平均时延为：

$$T_{\mathrm{PBFT}}=T_v+T_a+\frac{3S^{\mathrm{B}}\lg n}{R_t} \tag{11}$$

式中，T_v为区块验证时延；T_a为区块排队等待时延；R_t为数据传输速率。由于网络存在时延，单个分片内的交易需要等待一段时间才能获得最终确认以实现全网的一致性。为了尽可能保持区块链账本的一致性并防止区块在进入最终共识之前被丢弃，共识阶段的交易处理时延应限制在一定的区块成块间隔内，那么交易的共识时延应该受到以下约束：

$$T_{\mathrm{PBFT}}\leqslant\gamma T_{\mathrm{I}}\quad 0<\gamma<1 \tag{12}$$

2.2　分片优化问题

在本文中，分片区块链性能优化的目的是在满足安全性约束和交易共识时延约束的条件下，尽可能最大化交易吞吐量。因此，结合约束式 (8)、式 (12)，建立分片区块链优化求解问题 P1：

$$\mathrm{P1}:\max_{N_s,S^{\mathrm{B}},T_{\mathrm{I}}}\sum_{i=1}^{N_{\mathrm{s}}}\left\lfloor(S^{\mathrm{B}}-S_{\mathrm{H}}^{\mathrm{B}})/\beta\right\rfloor/T_{\mathrm{I}} \tag{13}$$

$$\text{s.t. 式(8),式(12)}$$

由于区块链配置参数复杂以及存在非线性约束，解决上述优化问题非常困难。

本文假设每个节点具有相同的交易处理能力，每个节点处的交易处理时延相等。同时，假设恶意节点均匀分布在每个分片中，则每个分片内的交易吞吐量一致。由式 (10) 可知，当区块大小S^{B}和区块成块间隔T_{I}确定的情况下，分片的数目N_{s}越大，则网络交易吞吐量TH越高。

当网络中总的恶意节点数满足 PBFT 共识算法的条件，即$N \geqslant 3M+1$时，在给定网络节点数目N、恶意节点数目M的情况下，约束条件式 (8) 可以转化为：

$$\frac{N}{N_{\mathrm{s}}} \geqslant 3\left\lceil \frac{M}{N_{\mathrm{s}}} \right\rceil + 1 \tag{14}$$

因此，P1 的优化问题可以转化成：

$$\mathrm{P2}: \max_{N_{\mathrm{s}}} N_{\mathrm{s}} \tag{15}$$

$$\text{s.t. 式}(12), \text{式}(14)$$

$$N_{\mathrm{s}} \geqslant 1，\text{且} N_{\mathrm{s}} \text{为整数}$$

对于优化问题 P2，在给定的假设条件下，很容易找到满足安全性约束的最优分片数目N_{s}^{*}，使得系统的交易吞吐量最大。但由于每个节点的行为 (恶意或诚实) 是完全不可知的，要使恶意节点能均匀分布于各个分片比较困难。因此，本文提出了一种基于演化博弈的分片选择算法来处理此问题。

3 基于演化博弈的节点分片选择

采用 PBFT 共识算法的分片区块链网络可以保证数据的最终一致性，但分片内恶意节点的随机分布导致某些分片内交易共识有效性遭到破坏，从而影响这些分片的性能。本节在不牺牲系统可扩展性和安全性的前提下，设计节点分片选择算法，以使恶意节点尽可能均匀地分布在每个分片中。

3.1 节点分片选择的演化博弈问题

区块链网络对每个节点的行为是完全不可知的，且每个节点不能掌握全局所有节点的信息，只能获取自己及邻居节点的部分信息。所以，在进行分片选择时，节点只能依靠这些不完全信息来给出决策。其次，考虑到节点是有限理性的，因此，节点无法一次性给出全局最优的分片选择策略。最后，由于区块链网络是一个分布式系统，不存在中央控制节点，因此，无法对分片的选择进行全局控制。

目前，演化博弈理论被认为是研究分布式网络中的有限理性节点决策行为的有效工具[20]。与传统博弈模型不同，在演化博弈过程中，节点不断与周围邻居节点进行博弈，通过多次试错达到博弈均衡。同时，演化博弈不要求节点是完全理性的且不需要掌握全局信息，本节将共识节点的分片选择过程建为演化博弈模型$\mathcal{G}=\{\mathcal{N},\mathcal{S},\boldsymbol{x},\boldsymbol{y}\}$，其中：

1) $\mathcal{N}$为参与分片选择的所有共识节点集合，$|\mathcal{N}|=N$。

2) $\mathcal{S}=\left\{S_1,S_2,\cdots,S_{N_{\mathrm{s}}^{*}}\right\}$是分片的集合，每个共识节点将选择加入到一个分片$S_i$中，$S_i \in \mathcal{S}$。

3) $\boldsymbol{x}=[\{x_1^{\mathrm{h}},x_1^{\mathrm{m}}\},\{x_2^{\mathrm{h}},x_2^{\mathrm{m}}\},\cdots,\{x_{N_{\mathrm{s}}^{*}}^{\mathrm{h}},x_{N_{\mathrm{s}}^{*}}^{\mathrm{m}}\}]^{\mathrm{T}}$为分片内节点数目的状态矢量。式中，$x_i^{\mathrm{h}}$代表分片$S_i$内诚实节点在全网的占比；$x_i^{\mathrm{m}}$代表分片$S_i$内恶意节点在全网的占比；且$\sum_{S_i\in\mathcal{S}} x_i^{\mathrm{h}}=N-M$及$\sum_{S_i\in\mathcal{S}} x_i^{\mathrm{m}}=M$。

4) $\boldsymbol{y}=[\{y_1^{\mathrm{h}},y_1^{\mathrm{m}}\},\{y_2^{\mathrm{h}},y_2^{\mathrm{m}}\},\cdots,\{y_{N_s^{*}}^{\mathrm{h}},y_{N_s^{*}}^{\mathrm{m}}\}]^{\mathrm{T}}$为分片内节点的收益矢量，式中，$y_i^{\mathrm{h}}$代表分片$S_i$内诚实节点的收益；$y_i^{\mathrm{m}}$代表代表分片$S_i$内恶意节点的收益。

3.2 收益函数

在演化博弈中，收益函数对节点做出决策起着至关重要的作用，每个共识节点在做决策时都倾向于选择使自身收益最大化的策略。因此，本节在设计节点收益函数，使具有有限理性的共识节点在进行分片选择时，选择使自己收益最大化的分片，能最终逐步达到均衡点。

共识节点的收益不仅取决于其策略，同时还取决于同分片内其他共识节点的行为，即分片内当前节点的状态。此外，PBFT 共识算法要求分片内诚实节点至少占分片内总节点的三分之二，才能对交易成功达成共识，并产生区块。假设在一个时间周期T内，分片内成功产生的预期区块数目被定义为变量k的连续可微单调递增函数$f(\theta)$，θ为分片内诚实节点的比例，$f(0)=0$。分片S_i在时间周期T内产生的预期区块数目为$f(\theta_i)$，其中分片S_i内诚实节点的比例为θ_i：

$$\theta_i = \frac{x_i^{\mathrm{h}}(N-M)}{x_i^{\mathrm{h}}(N-M)+x_i^{\mathrm{m}}M} \tag{16}$$

当成功产生一个区块后，区块链网络为参与成块的所有共识节点提供奖励R，R为该新区块内交易的总费用及产生区块的奖励之和。每个参与共识

的节点单独获得的奖励r为：

$$r=\frac{R}{x_i^h(N-M)+x_i^m M} \tag{17}$$

如果分片内共识节点未成功对交易达成共识，系统会在超时后提出一个空的区块，参与该轮共识的所有节点都没有奖励。

其次，假设诚实节点参与共识的成本为e，恶意节点表现出不合作行为，即不参与共识，其共识成本为0。因此，在时间周期T内，对于分片S_i内诚实节点的收益为：

$$y_i^h=rf(\theta_i)-e \tag{18}$$

分片S_i内恶意节点的收益为：

$$y_i^m=rf(\theta_i) \tag{19}$$

3.3　演化更新

在每一轮博弈后，节点随机选择邻居分片内的某一节点进行收益比较，并在收益较低时以概率W在下一轮博弈转入到其他分片中。策略转变的概率W采用统计物理中的费米函数来计算。也就是说，分片S_i的节点N_i随机选择分片S_j内的节点N_j进行收益比较，在下一轮该节点N_i选择分片S_j的概率为：

$$W(S_i\to S_j)=\frac{1}{1+\exp^{-(y_j-y_i)/\delta}} \tag{20}$$

如果分片切换概率$W(S_i\to S_j)$大于门限ω，则在下一轮，节点N_i切换到分片S_j，否则不变。算法 1 描述了包含N个共识节点的区块链网络遵循费米规则进行分片选择的演化博弈过程。

算法 1：基于演化博弈的节点分片选择

初始化：对于所有的节点$N_i\in\mathcal{N}$，随机选择一个分片$S_i\in\mathcal{S}$开始；

输入：$t\leftarrow 1$

while 分片内的节点未收敛或$t<\mathrm{T}_{\max}$ do

　for $N_i\in\mathcal{N}$ do

　　随机选择一个分片$S_j\in\mathcal{S}$；

　　计算节点N_i和分片S_j内的随机节点N_j在本轮博弈的收益y_i和y_j；

　　根据式 (20) 计算概率$W(S_i\to S_j)$；

　　if $W(S_i\to S_j)>\omega$ do

　　节点N_i在下一轮切换到分片S_j；

　　else

　　节点N_i保持继续在分片S_i内；

　　end if

　$t\leftarrow t+1$

　end for

end while

4　实验结果

为了验证本文提出的算法能够有效解决分片区块链的可扩展性和安全性均衡问题，同时能解决恶意节点分布不均的问题，本节进行数值仿真分析。

4.1　仿真参数配置

在性能理论分析中，本文均假设系统中每个节点都具有相同的交易处理能力，且每个节点上的交易处理时延一致。区块链网络的交易速率为平均每秒 50 笔，除非另有说明，否则仿真参数如表 1 所示。

表 1　仿真参数

参数设置	参数值
网络节点数N/个	1 000
恶意节点数目K/个	100～250
区块大小S^{B}/MB	50
区块间隔T_{I}/s	1
时延阈值参数γ	1/6
消息的验证时间T_v/s	0.1
区块排队时延T_a/s	0.2
数据传输速率R_t/Mbps	10
区块头大小$S_{\mathrm{H}}^{\mathrm{B}}$/B	10
交易平均大小β/B	64
共识代价e	1/10
成块奖励R	20
门限切换概率ω	0.5

4.2　分析模型验证

通过分析在不同网络参数下的网络性能随分片数目的变化情况，来验证本文提出的分析模型的有效性。

仿真实验中设置分片数目为 10～100 个，步长为 10 个，恶意节点数目分别设置为$M=[100,150,200,250]$。恶意节点随机加入到任意分片中，然后根据式 (4) 计算分片内交易失效的概率。图 1 展示了网络包含不同恶意节点数目下的分片交易失效概率。图 1 表明，当网络恶意节点数为 100 个、分片数目小于 50 个时，分片内交易失效概率低于 2%。同时，当网络中包含的恶意节点数目一定时，分片数目越多则交易失效概率缓慢上升。此外，还可看

到，交易的失效概率随着网络包含的恶意节点数目的增加而增长。这是由于随着越来越多新的恶意节点加入网络，单个分片内可能的恶意节点数目随之变多，导致交易共识失败，这符合理论模型的分析。

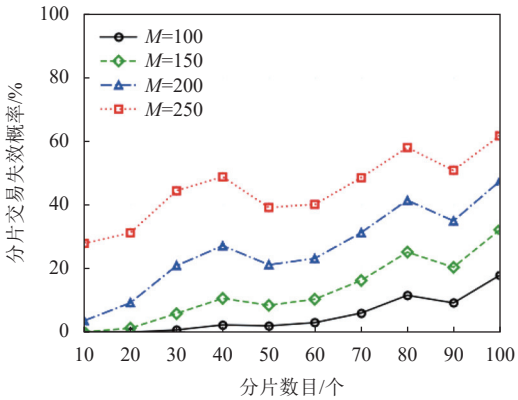

图 1 不同分片数目下的交易失效概率

其次，实验分析了不同分片数目对交易吞吐量和交易共识时延的影响。实验设置网络的节点数目为$N=1\,000$个，恶意节点数占比 10%，即$M=100$个。区块大小分别设置为$S^{\mathrm{B}}=[50,100,150,200]$ MB。图 2 为区块大小逐渐增加时的交易平均共识时延。从中可以看出，交易平均共识时延与区块大小和分片数目有关，区块越大则平均时延越高，因为其增加了交易打包到区块的排队时延。

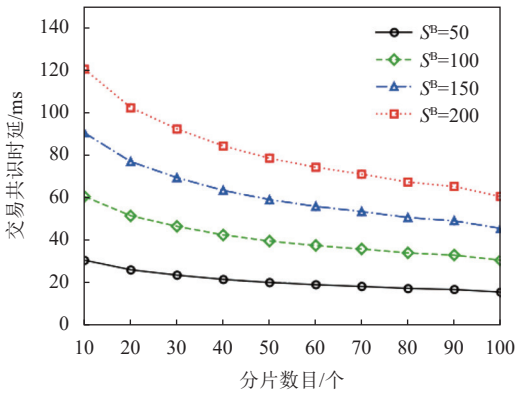

图 2 不同分片数目下的共识时延

图 3 给出了分片数目对网络交易吞吐量的影响，区块大小分别设置为$S^{\mathrm{B}}=50$ MB，恶意节点数目$M=[100,150,200,250]$。其表明网络交易吞吐量随着分片数目的增加而有效地增长。但当网络恶意节点数目大于 200 个、分片数目超过 90 个时，网络交易吞吐量反而下降。这是由于过多的分片数目导致某些分片内包含的恶意节点超过 PBFT 共识算法的安全性要求，导致分片共识失败。

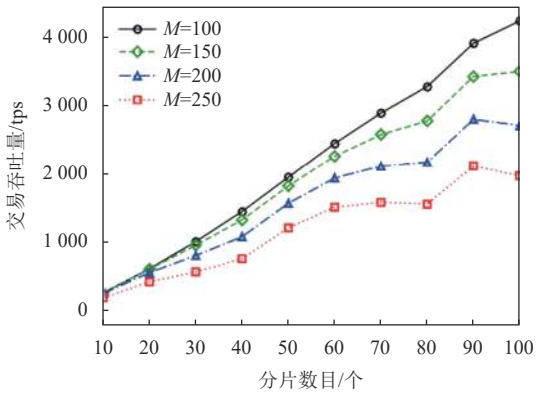

图 3 不同分片数目下的交易吞吐量

4.3 演化收敛性分析

分析基于演化博弈的节点分片选择算法的收敛性，实验设置分片数目为$N_{\mathrm{s}}=4$个，共识代价为$e=0.01$，每成功产生一个新区块的成块奖励$R=0.5$。演化更新的博弈间隔为$T=60$ s，$f(\theta)=\ln(1+\theta)$。初始时刻，恶意节点在每个分片内的占比为$[x_1^m,x_2^m,x_3^m,x_4^m]=[0.5,0.3,0.2,0]$。

图 4 和图 5 分别给出了 4 个分片内，恶意节点占比和诚实节点占比的动态演化过程。从图 4 和图 5 可以观察到，不同类型的节点在全网的占比随着时间的推移逐渐达到平衡点并稳定下来，最后每个分片内的不同类型节点的占比都接近一致。因此，其证明了本文提出的演化博弈分片选择算法具有收敛性，且能使有限理性的节点最后大概均匀分布于每个分片。

图 6 展示了每个分片内节点的平均收益，在演化初期，由于第四个分片全为诚实节点，共识的成功率较高，使得该分片内的节点平均收益高于其他 3 个分片。随着博弈演化，越来越多的恶意节点转移到第四个分片，第四个分片的平均收益逐渐减少，而其他分片的平均收益增加。最后，每个分片内的平均收益都达到均衡，具有相同的平均收益。

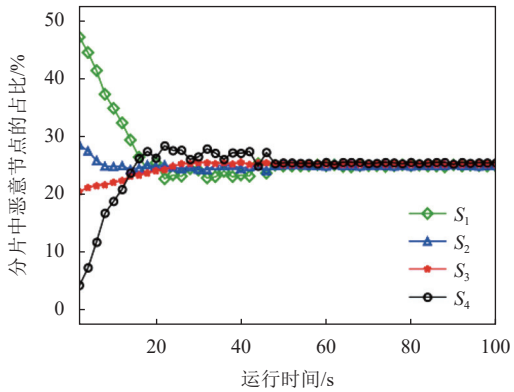

图 4 分片内恶意节点占比的动态演化

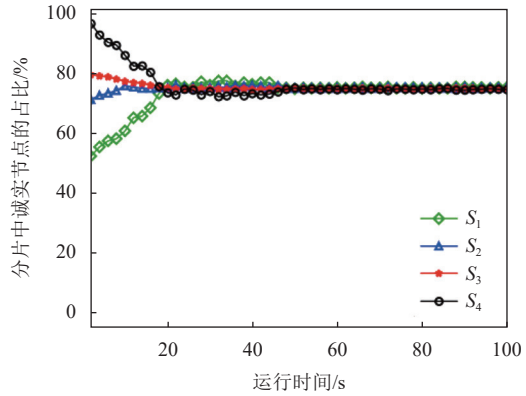

图 5　分片内诚实节点占比的动态演化

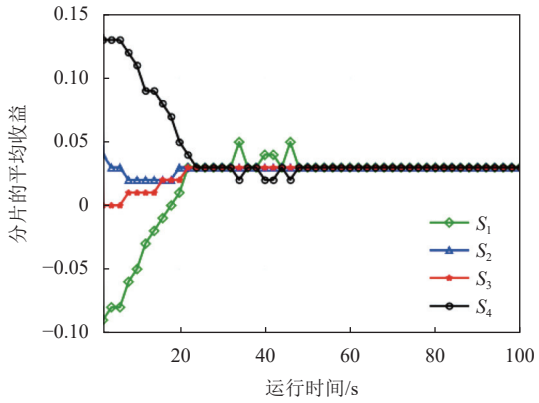

图 6　分片节点的平均收益的动态演化

4.4　性能对比分析

将提出的基于演化博弈的分片算法 (用 EGT-Based 表示) 与 Elastico 算法[12]、OmniLedger[13] 算法进行性能比较，对比的指标包括交易吞吐量和分片切换时延。实验设置网络中恶意节点的占比为 10%，分片数目为$N_s=[1,2,4,8,16]$。OmniLedger 算法中无偏差随机数生成方案 RandHound 的参数 $c=16$。网络连接带宽设置为 20 Mbps，节点间通信链路时延为 100 ms。

图 7 给出了在不同分片算法下的分片切换时延对比结果。图 7 表明，随着分片数目增多，分片切换时延呈现近似线性的增长。其中，Elastico 算法的分片切换时延最长，1 个分片的时延为 109 s，16 个分片的时延为 743 s。这是因为在 Elastico 算法中，节点需要花费较多的时间求解 PoW 难题来加入分片，导致很高的时延。本文提出的 EGT-Based 算法的分片切换时延要略高于 OmniLedger 算法，主要由于演化博弈需要进行多轮才能达到均衡，节点需要和邻居节点多次通信，从而导致时延的上升。

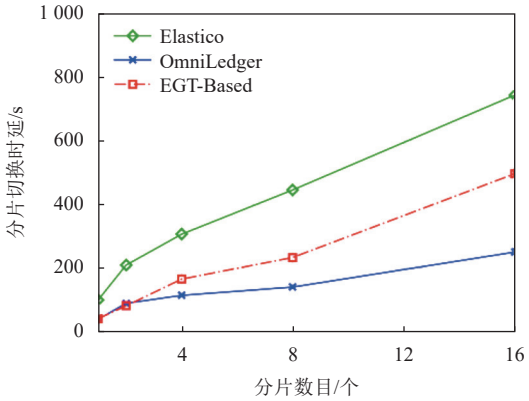

图 7　不同分片数目下的分片切换

图 8 给出了在不同分片算法下的网络交易吞吐量对比，可以看出，随着分片数目增加，本文提出的 EGT-Based 分片算法的交易吞吐量要明显优于其他两种算法。这是因为恶意节点均匀分布于每个分片，使得单个分片的失效概率接近于 0。而在 OmniLedger 算法中，RandHound 方案可能选择恶意节点担任主节点，造成分片的失败。同时，Elastico 算法太过频繁进行分片重构，引入较高的分片切换时延，会造成整体的交易吞吐量下降。

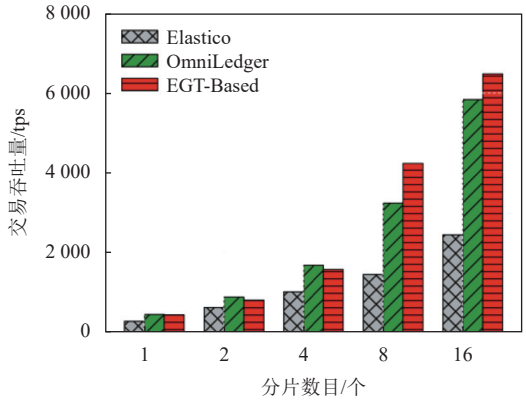

图 8　不同分片数目下的交易吞吐量

5　结 束 语

分片技术有望解决物联网区块链中可扩展性不足的问题。本文首先理论分析了分片区块链的分片安全性和可扩展性。其次，为了均衡分片区块链的可扩展和分片安全性，提出了一种基于演化博弈的分片算法来优化节点分片选择。实验结果表明，本文算法可以有效解决分片区块链中恶意节点分布不均导致的安全性问题，同时能提高网络的可扩展性。在未来的工作中，可以在分片区块链中考虑更多与动态环境相关的因素，如节点的动态加入和退出，将本文提出的基于演化博弈的区块链分片算法应用于真实的物联网中。

参 考 文 献

[1] SUN G, CHANG V, RAMACHANDRAN M, et al. Efficient location privacy algorithm for Internet of things (IoT) services and applications[J]. Journal of Network and Computer Applications, 2017, 89: 3-13.

[2] 杨毅宇, 周威, 赵尚儒, 等. 物联网安全研究综述: 威胁, 检测与防御[J]. 通信学报, 2021, 42(8): 187-205.
YANG Y Y, ZHOU W, ZHAO S R, et al. Survey of IoT security research: Threats, detection and defense[J]. Journal of Communications, 2021, 42(8): 187-205.

[3] ZHOU W, JIA Y, PENG A, et al. The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved[J]. IEEE Internet of Things Journal, 2018, 6(2): 1606-1616.

[4] LUO L, FENG J C, YU H F, et al. Blockchain-enabled two-way auction mechanism for electricity trading in Internet of electric vehicles[J]. IEEE Internet of Things Journal, 2021, DOI: 10.1109/JIOT.2021.3082769.

[5] KAUR K, G KADDOUM, ZEADALLY S. Blockchain-based cyber-physical security for electrical vehicle aided smart grid ecosystem[J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(8): 5178-5189.

[6] XU X Q, WANG X N, LI Z H, et al. Mitigating conflicting transactions in hyperledger fabric permissioned blockchain for delay-sensitive IoT applications[J]. IEEE Internet of Things Journal, 2021, 8(13): 10596-10607.

[7] HUANG H, YUE Z, PENG X, et al. Elastic resource allocation against imbalanced transaction assignments in sharding-based permissioned blockchains[J]. IEEE Transactions on Parallel and Distributed Systems, 2022, DOI: 10.1109/TPDS.2022.3141737.

[8] XIE J F, YU F, HUANG T, et al. A survey on the scalability of blockchain systems[J]. IEEE Network, 2019, 33(5): 166-173.

[9] CAI X, GENG S, ZHANG J, et al. A sharding scheme based many-objective optimization algorithm for enhancing security in blockchain-enabled industrial Internet of things[J]. IEEE Transactions on Industrial Informatics, 2021, 17(11): 7650-7658.

[10] LIU M, YU F R, TENG Y, et al. Performance optimization for blockchain-enabled industrial Internet of things (IoT) systems: A deep reinforcement learning approach[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3559-3570.

[11] XU X Q, SUN G, YU H F. An efficient blockchain PBFT consensus protocol in energy constrained IoT applications[C]//2021 International Conference on UK-China Emerging Technologies (UCET). Chengdu: IEEE, 2021: 152-157.

[12] LUU L, NARAYANAN V, ZHENG C, et al. A secure sharding protocol for open blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Austria: ACM, 2016: 17-30.

[13] KOKORIS 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.

[14] DANG H, DINH T, LOGHIN D, et al. Towards scaling blockchain systems via sharding[C]//Proceedings of the 2019 International Conference on Management of Data. Netherland: ACM, 2019: 123-140.

[15] ZAMANI M, MOVAHEDI M, RAYKOVA M. Rapidchain: Scaling blockchain via full sharding[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2018: 931-948.

[16] HAFID A, HAFID A S, SAMIH M. A methodology for a probabilistic security analysis of sharding-based blockchain protocols[C]//International Congress on Blockchain and Applications. Avila: Springer, 2019: 101-109.

[17] HAFID A, HAFID A S, SAMIH M. New mathematical model to analyze security of sharding-based blockchain protocols[J]. IEEE Access, 2019, 7: 185447-185457.

[18] XU X Q, SUN G, LUO L, et al. Latency performance modeling and analysis for hyperledger fabric blockchain network[J]. Information Processing & Management, 2021, 58(1): 102436.

[19] ZHANG J, HONG Z, QIU X, et al. SkyChain: A deep reinforcement learning-empowered dynamic blockchain sharding system[C]//49th International Conference on Parallel Processing-ICPP. Canada: ACM, 2020: 1-11.

[20] MAI T, YAO H, ZHANG N, et al. Cloud mining pool aided blockchain-enabled Internet of things: An evolutionary game approach[J]. IEEE Transactions on Cloud Computing, 2021, DOI: 10.1109/TCC.2021.3110965.

编 辑 刘飞阳