联合分布算法对区块链分片的稳定性分析优化研究

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，昆明 650500)

摘　要：在基于 Hyperledger Fabric 架构的区块链网络中，可以通过分片来提高吞吐量. 在分片之前，需要预先评估每个委员会的失败概率，以获得更稳定的分片方案. 本文提出了一种联合分布(JD)算法. 首先，对于预分片方案中的节点，根据预分片方案中的委员会数量进行随机抽样，然后得到每个委员会中节点的超几何分布；其次，根据节点的超几何分布计算每个委员会中恶意节点的概率，并根据这些概率构建所有委员会的联合分布函数；最后，根据各委员会的联合分布函数，计算整个分片方案的失败概率和失败年数，实现区块链分片的稳定性评估. 仿真结果表明，通过计算 Wilson 置信区间验证了计算失败概率的准确性，与 RapidChain 的分片稳定性分析算法和 Hoeffding 边界算法相比，联合分布(JD)算法可以更好地估计区块链分片的稳定性.

关键词：区块链；分片；稳定性；联合分布
中图分类号：TP305　　**文献标识码**：A　　DOI：10.19907/j.0490-6756.2022.032001

Optimization of security of Blockchain sharding by joint distribution algorithm

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

Abstract: The throughput can be improved by sharding in the blockchain network based on Hyperledger Fabric architecture, before sharding, it is required to pre-evaluate the failure probability of each committee, so as to obtain a more stable sharding scheme. This paper proposes a joint distribution (JD) algorithm. Firstly, for the nodes in the pre sharding scheme, random sampling is performed according to the number of committees in the pre-sharding scheme, the hypergeometric distribution of nodes in each committee is then obtained. Secondly, the probability of malicious nodes in each committee is calculated according to the hypergeometric distribution of nodes, and the joint distribution function of all committees is constructed according to these probabilities. Finally, according to the joint distribution function of all committees, the failure probability and failure years of the whole sharding scheme are calculated to realize the stability evaluation of blockchain sharding. The simulation results show that the accuracy of calculating the failure probability is verified by calculating Wilson confidence interval, which is compared with RapidChain's sharding stability analysis algorithm and Hoeffding boundary algorithm, Joint distribution (JD) algorithm can better estimate the stability of blockchain sharding.

Keywords: Blockchain; Sharding; Stability; Joint distribution

收稿日期：2021-03-10
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，主要从事数据挖掘、数据分析、区块链等研究. E-mail：liuyun@kmust.edu.cn
通讯作者：朱鹏俊. E-mail：1728137634@qq.com

1　引　言

基于 Hyperledger Fabric 架构的区块链网络可以通过分片实现吞吐量的提高,但分片会降低区块链的稳定性,因此需要在分片前针对各个委员会失败概率进行预评估,得到具有较高稳定性的分片方案[1-6].

Hafid 等提出的使用 Hoeffding 边界算法分析区块链协议的稳定性,计算单个委员会的失败概率并乘以委员会数量得到分片失败概率的精确边界,适用于二项分布和超几何分布的随机变量[7]. Zamani 等提出了一种 RapidChain 方案,其中的稳定性分析算法使用超几何分布对分片节点进行建模采样,能准确地计算单个分片失败概率,但在计算整体分片失败概率时存在一定局限性[8].

为了能够更好地分析区块链分片的稳定性,提出了一种基于 Hyperledger Fabric 架构下区块链分片的联合分布(Joint Distribution,JD)算法. 首先,针对预分片的节点,按预分片方案的委员会数量进行不放回的随机抽样,从而获得每个委员会中节点的超几何分布;其次,根据节点的超几何分布计算每个委员会中含有恶意节点的概率 ,并构建所有委员会的联合分布函数;最后,根据所有委员会的联合分布函数计算整个分片方案的失败概率和失败年限,从而提高区块链分片稳定性分析的精准度.

2　分片模型与稳定性评估

2.1　分片模型

分片的核心思想就是将节点划分为不同的委员会[9],为了构建图 1 的分片模型,假设初始输入的网络节点总数为 N,其中包括 $M(M<N)$ 个恶意节点. 在分片时,根据输入的各种节点数和预计分片的委员会数计算分析区块链分片的稳定性参数. 根据参数对分片稳定性进行评估,若预分片的稳定性较低,则需要改变单个委员会的节点数量以提高分片的稳定性,直到稳定性达到要求即可确定最终分片方案中的委员会节点数 n. 在分片形成时,分片算法根据委员会节点数 n 形成 λ 个委员会,其中委员会数量 $\lambda=M/n$,并将区块链中的诚实节点和恶意节点分配至各个委员会中,其中,第 $i(i=1,2,\cdots,\lambda)$ 个委员会分进 m_i 个恶意节点和 $n-m_i$ 个诚实节点,其中 $M=\sum_{i=1}^{\lambda} m_i$.

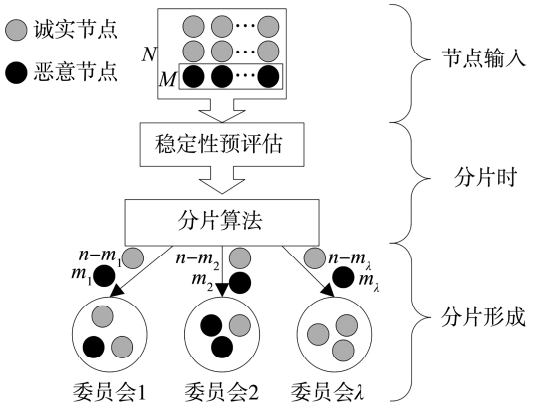

图 1　分片模型

Fig. 1　Sharding model

在分片模型中,将评估分片的稳定性量化为测量分片失败概率和分片失败年限等参数[10],分片的失败概率越低、失败年限越长,分片的稳定性越好;反之稳定性越差.

2.2　稳定性参数测量模型

在基于分片的区块链协议中,分片中若存在至少一个委员会被破坏,则整个区块链网络就会被破坏,即单分片接管攻击[11]. 因此完成一次分片的失败概率 f_p 是指在一次分片中至少有一个委员会失败的概率,平均失败年限 Y_f 则是根据失败概率和每年的分片次数进行计算的平均年限.

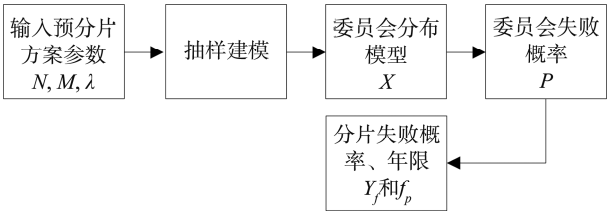

图 2　稳定性参数测量的主要流程

Fig. 2　The main flow of the stability parameter measurement

稳定性参数通常是按图 2 模型的顺序进行计算,模型的输入为预分片方案的参数 N,M,n. 首先,根据输入的参数对节点进行建模抽样,获得单个委员会的分布模型 X_i;其次,通过单个委员会的分布计算出所有委员会的整体失败概率 P,并根据委员会弹性 r 以及区块链整体弹性 R 获得委员会中恶意节点数的所有情况;最后,可以计算出完成一次分片的失败概率 f_p 和平均失败年限 Y_f. 在得出这两个参数后,分析失败概率 f_p 和失败年限 Y_f 是否满足分片稳定性要求,若分片失败概率过高、失败年限过短会导致分片的稳定性不高,容易被恶意节点攻击,需要改变委员会节点数 n 以提高分片

的稳定性.

除前文中定义的参数，另外还定义了一些名词属性，如下.

定义 1　委员会弹性 r：委员会在安全情况下能够包含的恶意节点的最大百分比. 多数区块链分片协议中这个弹性为 33%[12,13]，在 RapidChain 区块链分片协议中这个弹性为 50%[8].

定义 2　区块链整体弹性 R：区块链在安全情况下能够包含的恶意节点的最大百分比. 多数区块链分片协议中这个弹性为 25%[12,13]，在 RapidChain 区块链分片协议中这个弹性为 33%[8].

3　联合分布(JD)算法

3.1　JD 算法

在区块链网络中，分配节点到委员会的过程可以建模成不放回的随机抽样. 目前常用的分片规范是基于二项分布的，无法正确建模采样. 当样本不放回时，分片中的采样与超几何分布相匹配，相比二项分布具有更好的逼近性[14]. 因此，本文提出的联合分布(JD)算法是基于超几何分布来分配节点至各个委员会中.

根据图 1 中的分片模型以及参数，按图 3 的流程计算分片失败概率和失败年限.

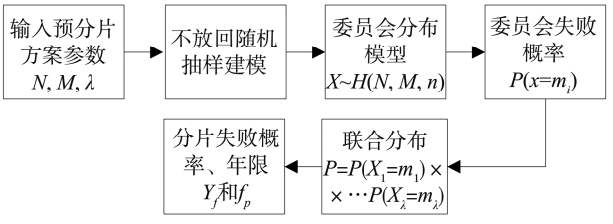

图 3　联合分布稳定性评估模型

Fig. 3　Joint distribution stability evaluation model

首先，对于输入的预分片方案，根据方案中的参数对所有节点进行不放回的随机抽样，构建各个委员会中节点的超几何分布. 在对第一个进行抽样后，抽样模型的参数 N 和 M 发生变化，N 变为 $N-n$，M 变为 $M-m_1$；当对第二个委员会采样后，参数 $N-n$ 变为 $N-2n$，$M-m_1$ 变为 $M-m_1-m_2$，直到对第 $\lambda-1$ 个委员会抽样后，参数变为 $N-(\lambda-1)n$ 和 $M-\sum_{i=1}^{\lambda-1}m_i$.

每个委员会的分布可以通过参数 N，M 和 n 的超几何分布建模，超几何分布的表达式如式(1).

$$X\sim H(N,M,n) \tag{1}$$

因此，根据式(1)，可以依次确切的构建每个委员会的分布模型，如式(2)为第一个委员会的分布.

$$X_1\sim H(N,M,n) \tag{2}$$

同样可以写出第二个，第三个委员会以及第 λ 个委员会的分布，如式(3)～(5).

$$X_2\sim H(N-n,M-m_1,n) \tag{3}$$

$$X_3\sim H(N-2n,M-(m_1+m_2),n) \tag{4}$$

$$X_\lambda\sim H(N-(\lambda-1)n,M-\sum_{i=1}^{\lambda-1}m_i,n) \tag{5}$$

根据每个委员会的分布，可以计算第一个至第 λ 个委员会中抽到 $m_i(i=1,2,\cdots,\lambda)$ 个恶意节点的概率. 则第一个委员会的概率和第 λ 个委员会的概率函数[15]分别为式(6)和式(7).

$$P(X_1=m_1)=h(N,M,n,m_1)=\frac{\binom{M}{m_1}\binom{N-M}{n-m_1}}{\binom{N}{n}} \tag{6}$$

$$P(X_\lambda=m_\lambda)=h\left(N-(\lambda-1)n,M-\sum_{i=1}^{\lambda-1}m_i,n,m_\lambda\right)=\frac{\binom{M-\sum_{i=1}^{\lambda-1}m_i}{m_\lambda}\binom{N-(\lambda-1)n-M+\sum_{i=1}^{\lambda-1}m_i}{n-m_\lambda}}{\binom{N-(\lambda-1)n}{n}} \tag{7}$$

联合各委员会的概率函数 $P(X=m_i)$，可推出 $X=(X_1,X_2,\cdots,X_\lambda)$，即 λ 个委员会的联合分布函数如式(8)所示.

$$\begin{aligned}P(X)&=P(X_1=m_1,X_2=m_2,\cdots,X_\lambda=m_\lambda)=\\&P(X_1=m_1)\times P(X_2=m_2)\times\cdots\times P(X_\lambda=m_\lambda)=\\&h(N,M,n,m_1)\times h(N-n,M-m_1,n,m_2)\times\\&\cdots\times h\left(N-(\lambda-1)n,M-\sum_{i=1}^{\lambda-1}m_i,n,m_\lambda\right)=\\&\prod_{j=0}^{\lambda-1}h\left(N-jn,M-\sum_{i=1}^{j}m_i,n,m_{j+1}\right)\end{aligned} \tag{8}$$

定理 3.1　设 $X=\{X_1,X_2,\cdots,X_\lambda\}$ 是一个随机向量，则 $X_i\sim H(N-(i-1)n,M-\sum_{i=1}^{i-1}m_i,n)$ 对所有 $i\in\{1,2,\cdots,\lambda\}$ 有式(9)[16]：

$$\prod_{j=0}^{\lambda-1}h\left(N-jn,M-\sum_{i=1}^{j}m_i,n,m_{j+1}\right)=\frac{\prod_{j=0}^{\lambda-1}\binom{n}{m_i}}{\binom{N}{M}} \tag{9}$$

根据定理 3.1，可以将式(8)中的复杂分布计算简化为式(10)，

$$P(X_1=m_1,X_2=m_2,\cdots,X_\lambda=m_\lambda)=\frac{\binom{n}{m_1}\binom{n}{m_2}\cdots\binom{n}{m_\lambda}}{\binom{N}{M}}=\frac{\prod_{j=1}^{\lambda}\binom{n}{m_j}}{\binom{N}{M}} \tag{10}$$

第一个委员会中的m_1个恶意节点可以假设以下值中的任意一个:$n,n-1,\cdots,1,0$. 同样,第二个委员会中的m_2恶意节点可以假设以下任意值:$n,n-1,\cdots,1,0$,以此类推,直到最后一个委员会. 因此,式(8)和式(10)中的分布只表示一种特定的结果. 为了计算所有可能的结果,即满足每个委员会中恶意节点数不超过委员会弹性限度,需要计算这些情况的联合超几何分布,表达式如下式(11).

$$P(X_1\leqslant nr,X_2\leqslant nr,\cdots,X_\lambda\leqslant nr)=\frac{1}{\binom{N}{M}}\sum_{m_1=0}^{nr}\sum_{m_2=0}^{nr}\cdots\sum_{m_\lambda=0}^{nr}\binom{n}{m_1}\binom{n}{m_2}\cdots\binom{n}{m_\lambda} \tag{11}$$

最后,分片失败概率(至少一个委员会失败的概率)可以表示为式(12).

$$f_p=1-P(X_1\leqslant nr,X_2\leqslant nr,\cdots,X_\lambda\leqslant nr) \tag{12}$$

在联合分布的计算过程中,计算出每个委员会的分布函数,消除了每个委员会失败概率不独立的问题,可以更加精准的估计出切片失败的概率. 但即使式(8)到式(10)的计算得到简化,式(12)中的概率仍然复杂难以计算,尤其是在考虑到大量的节点时,因此只能估计该概率,而不是精准计算.

但是在试验次数较大时,确切的故障概率(f_p)和估计的失败概率($\hat{f}_p$)之间的关系可以表示如式(13).

$$|f_p-\hat{f}_p|\xrightarrow{N_t\to+\infty}0 \tag{13}$$

其中,$\hat{f}_p=\frac{N_s}{N_t}$,$N_s$是分片失败的试验次数;$N_t$是实验次数.

因此可以通过估计的失败概率来较精准的得到准确失败概率,并能降低计算复杂度.

另外根据完成一次分片的失败概率f_p,可以计算分片的失败年限. 平均失败年数的计算如式(14).

$$Y_f=\frac{E_s}{N_{sy}} \tag{14}$$

其中,$E_s=\frac{1}{f_p}$为分片失败前的预期分片次数;N_{sy}为每年的分片次数.

3.2　算法估计性能分析

为了确定估计失败概率的准确性,选择计算最准确、最可靠的 Wilson 置信区间[17,18],如式(15).

$$n=u+v,\ p=u/n,$$
$$S=(p+\frac{Z_\alpha^2}{2n}-\frac{Z_\alpha^2}{2n}\sqrt{4n(1-p)p+Z_\alpha^2})/(1+\frac{Z_\alpha^2}{2n}) \tag{15}$$

其中,S 为 Wilson 置信区间算法公式;n 为样本总数;u 为诚实节点数;v 为恶意节点数;Z_α表示对应某个置信水平的统计量,如在 95%的置信水平下,$Z_\alpha=1.96$. 使用 Wilson 置信区间计算上下边界以更好地限制和估计失败概率.

Hafid 等[7]在分析和比较 Hoeffding,Chebyshev 和 Chvátal 边界计算区块链分片的失败概率时,使用 Hoeffding 边界计算的失败概率会较另两种更低,取 Hoeffding 边界为更好的分片失败概率近似值,可以更好的分析区块链分片协议的稳定性. 据此在本文中算法计算分片失败概率越小,失败年限越大越能说明算法能够提供更好的稳定性估计.

4　仿真分析

4.1　仿真环境

为了估算由 JD 算法计算的分片失败概率,使用了 NumPy Python 库进行实验,该库提供了数学函数和随机数生成器等. 另外,还使用 numpy.array()来建立一个包含 M 个恶意节点和 $N-M$ 个诚实节点的数组. 还使用了 numpy.random.choice()将节点进行随机分布,而无需在分片上替换这些节点. 在配备 i7-2677M CPU 1.80 GHz 和 6 GB RAM 的 PC 上运行实验.

4.2　置信区间

在 $N=1000$,$M=250$ 的区块链网络模型中,计算了在改变单个委员会中节点数 n 分别为 125,200,250 和实验次数N_t为10^4,10^5,10^6时使用 JD 算法的估计失败概率. 为了更好地限定和估计失败概率,也计算了在置信水平为 95%时的 Wilson 置信区间的上下限,这意味着,有 95%的正确率确定估计的失败概率能在 Wilson 的上下限之间. 表 1 数据显示计算的失败概率落在置信区间的上下限之间,验证了 JD 算法计算的分片失败概率是准确可靠的.

表 1　不同实验次数和委员会节点数的估计失败概率及 Wilson 置信区间

Tab. 1　Estimated failure probability and Wilson confidence interval for different experiment times and number of committee nodes

实验次数 N_t	委员会节点数 n	估计失败概率 f_p	Wilson 置信区间	
			下限	上限
10 000	125	1.06×10^{-1}	1.00×10^{-1}	1.12×10^{-1}
	200	9.40×10^{-3}	7.76×10^{-3}	1.14×10^{-2}
	250	1.60×10^{-3}	1.06×10^{-3}	2.71×10^{-3}
100 000	125	1.03×10^{-1}	1.01×10^{-1}	1.04×10^{-1}
	200	8.00×10^{-3}	7.53×10^{-3}	8.64×10^{-3}
	250	1.10×10^{-3}	8.15×10^{-4}	1.21×10^{-3}
1 000 000	125	1.05×10^{-1}	1.04×10^{-1}	1.06×10^{-1}
	200	7.70×10^{-3}	7.68×10^{-3}	8.01×10^{-3}
	250	1.00×10^{-3}	—	—

4.3　失败概率分析

为了评估算法计算的分片失败概率，我们在两种参数的场景下进行了实验：(a) $N=1000$，$M=250$，$N_t=10^6$；(b) $N=4000$，$M=1333$，$N_t=10^6$. 两种场景分别为两种主流区块链分片协议下能容忍的最大恶意节点数，若恶意节点占比更低，稳定性的分析效果会更好. 在场景(a)中改变单个委员会节点数量 $n=100\sim250$，在场景(b)中改变单个委员会节点数量 $n=30\sim500$ 时的分片估计失败概率，并与 Hoeffding 边界算法和 RapidChain 的分片稳定性分析算法进行了比较.

图 4(a)和(b)中总体显示，分片的失败概率会随单个委员会中的节点数 n 的增加而降低，这是因为委员会中节点数量的增加，恶意节点的占比容易降低，恶意节点接管分片的难度会增大，从而降低分片失败概率. 在场景(a)和(b)中当 n 较小时，Hoeffding 边界算法的走势较为陡峭，说明 Hoeffding 边界算法在委员会节点数较少时的准确性差. 在图 4(a)和(b)中能观察到 Hoeffding 和 RapidChain 都有失败概率超过 1 的时候，这是因为这两种算法都只计算了第一个委员会的失败概率并将其乘以委员会的数量，从而导致计算概率的不准确. 另外在场景(a)和(b)中，JD 算法计算的分片失败概率都较另外两种算法更低，且不会超过 1，这是因为 JD 算法采用了适当的概率分布来计算，相比之下 JD 算法提供了更好的分片失败概率估计.

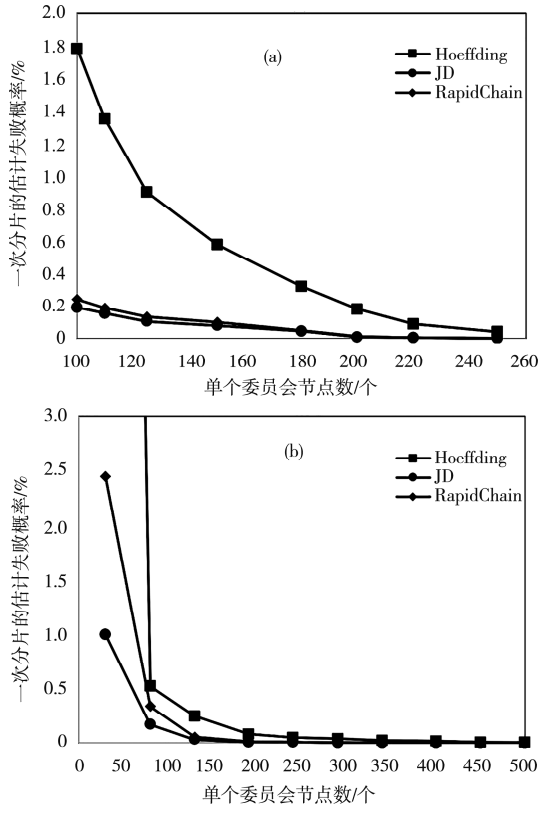

图 4　场景(a)和(b)中三种算法的失败概率

Fig. 4　The failure probability of three algorithms in scenario (a) and (b)

4.4　失败年限分析

评估算法计算的区块链分片的平均失败年限，在两种参数的场景下进行了实验：(a) $N=1000$，$M=250$，$N_t=10^6$；(b) $N=4000$，$M=1333$，$N_t=10^6$. 固定每年的分片次数，$N_{sy}=365$，计算在场景(a)中改变单个委员会节点数量 $n=100\sim250$，在场景(b)中改变单个委员会节点数量 $n=30\sim500$ 时的平均失败年限，并与 Hoeffding 边界算法和 RapidChain 的分片稳定性分析算法进行了比较.

图 5(a)和(b)中总体显示，随着委员会中节点数的增多，失败年限会升高，这是因为单个委员会的节点数增多，恶意节点在委员会中的占比就容易降低，分片越难以被攻击，使失败前的预期分片次数 E_s 增加，从而导致失败年限减少. 图 5(a)和(b)中 Hoeffding 边界算法计算的平均失败年限在随着委员会数量的增加时，并没有什么明显变化，说明 Hoeffding 边界算法在计算失败年限时的不准确；当 n 较小时，RapidChain 方法和 JD 算法计算的平均失败年限相差不大，但 n 逐渐变大时，JD 算法与 RapidChain 开始拉开差距，失败年限也开始远多于另外两种方案. 相比之下，JD 算法能够更好地确定分片的失败年限.

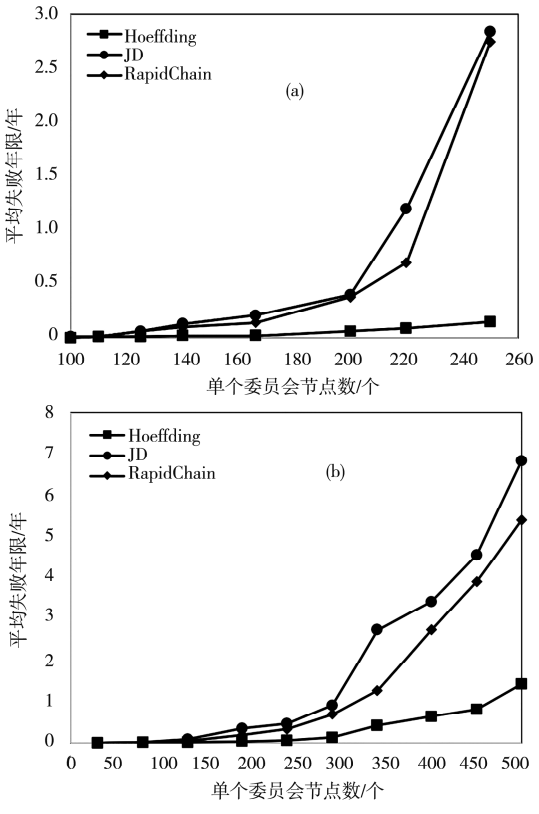

图 5　场景(a)和(b)中三种算法的平均失败年限

Fig. 5　Average failure years of three algorithms in scenarios (a) and (b)

5　结　论

区块链分片会降低区块链的稳定性,需要对分片进行稳定性预评估,得到具有较高稳定性的分片方案. JD 算法在计算分片失败概率和失败年限时能提供更好的估计,从而更好地分析区块链分片的稳定性. 算法首先针对预分片的节点,按预定委员会数量进行不放回的随机抽样,从而获得每个委员会中节点的超几何分布,其次根据节点的超几何分布计算每个委员会中含有恶意节点的概率,并构建所有委员会的联合分布函数,最后根据所有委员会的联合分布函数计算整个分片方案的失败概率和失败年限. 通过计算 Wilson 置信区间确定 JD 算法计算结果是正确的,另外仿真结果表明,JD 算法在计算分片失败概率和分片失败年限时有更好的估计,从而实现对分片稳定性的精准分析. 区块链分片是一个非常有挑战性的方向,在研究分片的稳定性问题之后,将着手进行区块链分片方案的研究,在保证区块链稳定性的同时尽可能提高其吞吐量.

参考文献:

[1]　Yu G, Wang X, Yu K, *et al*. Survey: sharding in blockchains [J]. IEEE Access, 2020, 8: 14155.

[2]　朱延杰, 张志生, 段琳. 主流开源区块链框架可扩展性分析[J]. 云南电力技术, 2018, 46: 26.

[3]　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.

[4]　朱建明, 张沁楠, 高胜. 区块链关键技术及其应用研究进展[J]. 太原理工大学学报, 2020, 51: 321.

[5]　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.

[6]　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.

[7]　Hafid A, Hafid A S, Samih M. A methodology for a probabilistic security analysis of sharding-based blockchain protocols [C]//Proceedings of the International Congress on Blockchain and Applications (Blockchain 2019). Cham: Springer, 2019.

[8]　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 (CCS'18). New York: ACM, 2018.

[9]　毛志来, 刘亚楠, 孙惠平, 等. 区块链性能扩展与安全研究[J]. 信息网络安全, 2020, 20: 56.

[10]　Dang H, Dinh T T A, Dumitrel L, *et al*. Towards scaling blockchain systems via sharding [C]// Proceedings of the 2019 International Conference on Management of Data. Amsterdam: ACM, 2019.

[11]　谭敏生, 杨杰, 丁琳, 等. 区块链共识机制综述[J]. 计算机工程, 2020, 46: 7.

[12]　Kokoris-Kogias E, Jovanovic P, Gasser L, *et al*. OmniLedger: a secure, scale-out, decentralized ledger via sharding [C]// Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP). San Francisco: IEEE, 2018.

[13]　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 (CCS'16). New York: ACM, 2016.

[14]　李玲. 常见概率分布间的极限关系[J]. 科技资讯, 2019, 17: 221.

[15]　Samohyl R W. Acceptance sampling for attributes via hypothesis testing and the hypergeometric distribution [J]. J Ind Eng Int, 2018, 14: 395.

[16]　Hafid A, Hafid A S, Samih M. A novel methodology-based joint hypergeometric distribution to analyze

the security of sharded blockchains [J]. IEEE Access, 2020, 8: 179389.

[17] Newcombe R G. Interval estimation for the difference between independent proportions: comparison of eleven methods [J]. Statist Med, 1998, 17: 873.

[18] Brown L D, Cai T T, Anirban D G. Interval estimation for a binomial proportion [J]. Stat Sci, 2001, 16: 101.

引用本文格式：

中　文：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.

英　文：Liu Y, Zhu P J, Chen L Y, *et al*. Optimization of security of Blockchain sharding by joint distribution algorithm [J]. J Sichuan Univ: Nat Sci Ed, 2022, 59: 032001.