DOI:10.19850/j.cnki.2096-4706.2023.04.007

基于节点属性分片的区块链研究设计

赵鹏，梁晋铭，刘佳宝
（太原师范学院，山西 晋中 030619）

摘　要：区块链系统的交易处理能力较弱使其无法广泛应用，分片是在不降低去中心化程度情况下解决区块链瓶颈的最佳技术，但目前主流的分片方案存在牺牲安全性来提升性能的问题。通过对现有分片方案进行研究，提出了基于节点属性的分片方案，根据节点属性和节点随机分配方法开展了网络分片、交易分片和状态分片。实验结果表明基于节点属性分片的区块链系统在满足系统安全的条件下提升了交易处理能力。

关键词：区块链；扩展性；节点属性；分片技术
中图分类号：TP311　　**文献标识码：**A　　**文章编号：**2096-4706（2023）04-0029-04

Research and Design of Blockchain Based on Node Attribute Fragmentation

ZHAO Peng, LIANG Jinming, LIU Jiabao
(Taiyuan Normal University, Jinzhong 030619, China)

Abstract: The weak transaction processing capability of blockchain system makes it unable to be widely used. Fragmentation is the best technology to solve the blockchain bottleneck without reducing the degree of decentralization. However, the current mainstream fragmentation scheme has the problem of improving performance at the expense of security. Based on the research of existing fragmentation schemes, a fragmentation scheme based on node attributes is proposed. According to node attributes and node random allocation method, network fragmentation, transaction fragmentation and state fragmentation are carried out. The experimental results show that the blockchain system based on node attribute fragmentation improves the transaction processing ability under the condition of meeting the system security.

Keywords: blockchain; extensibility; node attribute; fragmentation technology

0 引　言

区块链在交易处理和数据存储方面难以与中心化应用媲美，为了提高区块链的交易处理能力和可扩展性，一些学者提出运用分片技术来提升区块链的性能。Luu[1] 等人提出第一个公有链分片协议 Elastico，借鉴数据库分片的方式将区块链进行分片，将众多节点划分到不同的委员会，多个委员会并行处理事务提升区块链的交易处理能力。但 Elastico 在没有状态分片的前提下要求每经过一轮共识之后重新组织委员会，当网络中的节点数增多时，委员会重组会耗费大量的时间，进而导致区块链的 TPS 下降。Kokoris-Kogias 等人提出了一种抗预测的公共随机协议 Omniledger[2] 对区块链系统中的节点进行随机分片，引入一种有效的跨分片提交协议来处理跨分片的交易。Omniledger 在处理跨片交易时会将跨片交易广播给所有分片，由对应分片来进行验证，交易验证合法则生成有效证明，否则生成拒绝证明。但如果区块链系统的大部分分片中均有超过半数的跨片交易，则会产生大量的通信开销，进而造成 TPS 的下降，而节点有时并不能被均匀分配。Wang 等人提出 Monoxide[3] 协议，协议中提出了“异步共识组”的概念，采用“连弩挖矿”机制即一个矿工可以同时对多个分片挖矿，只要解决一次 PoW 难题便可打包多个分片的交易上链，相当于扩大了每个分片的算力，同时提出了“最终原子性”原则，在跨分片交易中将一笔转账分为扣款和存款，如果扣款操作被成功执行，在接收到接力交易后存款操作也将被成功执行。但由于区块链中的数据是永久储存的，随着区块链系统的运行，累计的交易数据会越来越多，相应的各节点的存储压力也会越来越大，有可能造成单点过热的问题。

本文基于节点属性的不同提出一个安全高效的分片方案，并将该分片方案应用到区块链系统中，研究表明在满足系统安全的前提下该方案可以提升基于区块链系统的交易处理能力。

1 基于节点属性分片的区块链设计

1.1 节点属性的设计

本文将 PoS 算法思想作为节点身份的验证机制，用代币资源替换算力资源，将节点自身利益与整个系统绑定，从而抵抗女巫攻击，同时赋予节点不同属性，不同属性的节点有不同功能，如静态属性节点分为存储节点和事务节点，存储节点负责存储区块链系统中的数据，事务节点负责交易的产生发布，所有静态属性节点负责动态属性节点的分配验证工作，动态属性节点负责验证交易的合法性和区块的共识等，用户通过身份验证机制进入区块链系统后，便可根据自身需求选择节点属性，进而参与系统的运行。

1.2 网络分片的设计

1.2.1 节点随机分配方法

针对节点分配不均、恶意节点伪造分片结果的问题，本

收稿日期：2022-09-22

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

文提出可验证随机函数 VRF 与一致性哈希算法相结合的节点随机分配方法，在保证可验证随机性的同时利用一致性哈希算法的特点，把节点均匀地分布在各分片中，节点的分配工作不依赖于某个委员会且避免了分片结果在全网广播，具体方法如下：

首先计算各分片在 Hash 环上的映射，然后节点在本地通过 VRF 算法计算出一个可验证的随机数，再使用该随机数结合一致性哈希算法得到节点在 Hash 环上的映射，从而得出节点所属的分片。为了能将节点均衡地分配到各分片，引入一致性哈希算法的虚拟节点机制，即对同一个分片取多个命名，分别计算各个命名在哈希环的映射，这样同一个分片就会在哈希环上有多个映射，从而保证节点随机并且均匀地分配在各分片中，如图 1 所示。

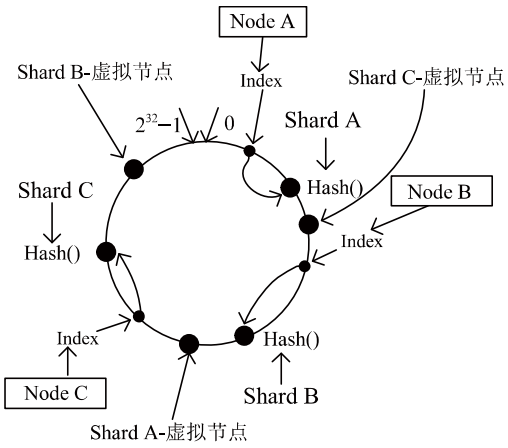


图 1 节点的均匀分配

若用节点某个关键值的 Hash 结果来分配节点，根据哈希函数相同输入必有相同输出的特性，节点每次分片均会被分到同一分片中。若用节点某个关键值与随机数进行一致性 Hash 结果来分配节点，虽然节点每次分片会被分配到不同分片中，但无法验证其结果是否由该节点产生，可能发生伪造现象。在本文提出的节点随机分配方法中，各分片委员会能通过 VRF 算法计算分配结果是否被伪造，还能依据其随机性避免某节点被重复分配到同一分片的情况，同时由单一委员会变为多个委员会并行分配节点，减少了节点分配所需时间。

1.2.2 重分片方法

区块链系统中即使有节点身份验证机制，但仍避免不了恶意节点的存在，而诚实节点长期处于某一分片可能会遭到恶意节点的腐败，进而转变为恶意节点，所以要保证节点进行周期性的重分片。但节点在参与共识之前要保证节点本地状态的一致性，因此重分片前后必须要保证各节点的本地状态一致以便能快速参与共识。在 Monoxide[3] 方案中，各分片完成一轮共识后由委员会将各分片产生的微区块聚合成完整的区块，再由全网同步该区块，达到各节点本地状态一致的目的。但节点同步全网的区块数据需要消耗较多的时间和带宽占用量，甚至造成网络拥塞，同时区块链系统运行时间越长，新节点启动时间（参与共识需要同步网络数据的时间）也越长。

针对重分片通信开销大和时耗时长的问题，在每个重分片周期结束前，各分片内产生的最后一个区块达成共识时，存储节点同步区块，同时动态属性节点在本地计算所属分片，并将结果与所需的检验凭证广播给所属静态属性节点委员会，静态属性节点委员会通过算法验证后，将节点纳入所属分片，即完成重分片。仅将动态属性节点重新随机分片，解决了重分片过程中同步区块数据带来的通信开销和节点的存储压力等问题，同时一个分片内有多个存储节点存储数据，避免了单点故障问题。

1.3 交易分片和状态分片的设计

交易分片指把系统中未确认的交易分配到相应的分片中进行处理，各分片并行处理交易，达到提高区块链交易处理能力的目的 [4]。区块链系统中的交易经由网络分片被分为片内交易和跨片交易。片内交易指交易双方均在同一个分片内，可以快速查询验证该交易是否合法，跨片交易指交易双方分别在不同的分片，在验证时就涉及该交易应交由哪个分片协助处理，如何减少处理跨片交易产生的通信开销等问题。目前主流交易分片方案中采用主链转发交易的方式完成对跨片交易的转发验证。如以太坊在其分片方案中设置了信标链对跨片交易进行转发，但若网络中存在大量交易时，单一的主链或者委员会却可能因为无法负载大量交易的转发工作而阻塞甚至崩溃，成为区块链系统的另一个瓶颈。

本文根据节点属性的不同提出新的交易分片方案。当网络分片完成后，各分片内的静态属性节点会临时记录当前分片内各节点的信息，事务节点在产生并发布交易后，存储节点和动态属性节点通过双方交易信息判断该交易的类别，如果是片内交易，则由动态属性节点验证交易的合法性，如果是跨片交易，则存储节点验证交易合法性后转发到相应分片，经由目标分片中的存储节点验证交易的合法性后交由动态属性节点进行验证。一个分片内的多个存储节点组成委员会并行转发和接收本分片的跨片交易，当目标分片的跨片交易数量达到规定值或收集时间超过规定值时，将交易切分后以并发的方式发送至目标委员会，来减少跨片交易转发时间，降低因跨片交易产生的通信开销。跨片交易示意图如图 2 所示。

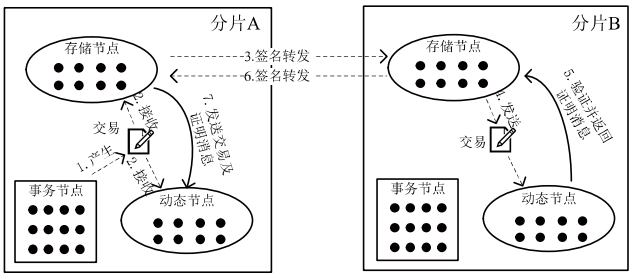


图 2 跨片交易示意图

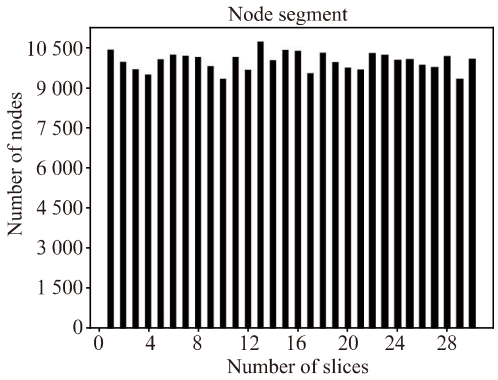
状态分片指将区块链系统中完整的交易数据分片存储，各分片存储、维护各自的交易数据，降低网络中节点的存储压力，减少网络中节点同步交易数据所消耗的时间。本文中各分片的交易数据由其内部的存储节点存储，所有的存储节点存储着区块链系统的数据信息，而存储节点不参与重分片过程，也就减少了状态分片中因重分片后数据同步导致的通信开销，从而形成了状态分片。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

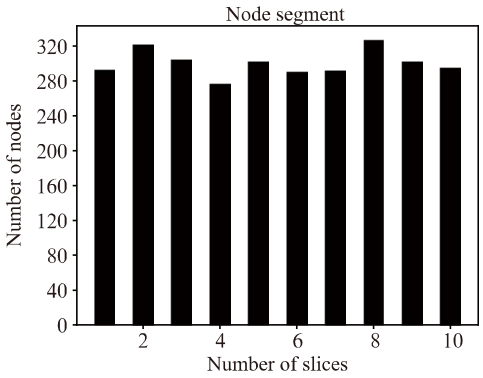
2　实验对比分析

2.1　节点均衡性分析

针对本文提出的网络分片方法将节点均衡分布情况作为指标对其分析。实验采用控制变量法，测试了分片数量和节点数量对节点均衡分布情况的影响。如图 3 所示本文提出的网络分片方案可以使节点均衡地分配在各分片，同时利用 VRF 函数的可验证性避免恶意节点伪造分片信息企图进入到某分片，提高了网络分片的安全性。



（a）节点在 30 个分片的分布情况图



（b）节点在 10 个分片的分布情况图

图 3　节点的分布情况图

2.2　安全性分析

本文提出的节点随机分配方法与随机抽样问题类似，因此采用超几何分布对网络分片的安全性进行分析。假设网络中总共有 N 个节点，其中有 M 个恶意节点，将节点平均划分为 k 个片区（$k \in Z^+$），每个片区内的节点数记为 $t=[N/k]$，每个片区内恶意节点数记为 X_k，以拜占庭类共识算法为例，PBFT 算法的容错率为 1/3，即每个分片内的恶意节点数少于片内总节点数的 1/3 时分片是安全的 [5]。

第一个分片中恶意节点数 m_1 服从超几何分布，因此第一个分片中恶意节点数 $X_1=m_1$ 的概率公式为：

$$P(X_1=m_1)=f(N,M,t,m_1)=\frac{C_{N-M}^{t-m_1}C_M^{m_1}}{C_N^t} \tag{1}$$

而分片中恶意节点数少于片内总节点数的 1/3 为安全，由此得出第一个分片安全的概率为：

$$P(X_1\leqslant\frac{t}{3})=\sum_{m_1=0}^{\frac{t}{3}}\frac{C_{N-M}^{t-m_1}C_M^{m_1}}{C_N^t} \tag{2}$$

第一个分片和第二个分片都安全的概率为：

$$P(X_1\leqslant\frac{t}{3},X_2\leqslant\frac{t}{3})=\sum_{m_1=0}^{\frac{t}{3}}\sum_{m_2=0}^{\frac{t}{3}}\frac{C_{N-M}^{t-m_1}C_M^{m_1}}{C_N^t}\frac{C_{N-t-M+m_1}^{t-m_2}C_{M-m_1}^{m_2}}{C_{N-t}^t} \tag{3}$$

同理，k 个分片都安全的概率为：

$$\begin{aligned}&P(X_1\leqslant\frac{t}{3},\ X_2\leqslant\frac{t}{3}\cdots X_k\leqslant\frac{t}{3})\\&=\sum_{m_1=0}^{\frac{t}{3}}\sum_{m_2=0}^{\frac{t}{3}}\cdots\sum_{m_k=0}^{\frac{t}{3}}f(N,M,t,m_1)f(N-t,M-m_1,t,m_2)\cdots\\&f(N-(k-1)t,M-\sum_{i=1}^{k-1}m_i,t,m_k)\end{aligned} \tag{4}$$

该联合概率计算较为复杂且难以计算，考虑到系统中有大规模节点的情况下，对其进行粗略的估算，本文使用了 Python 中的 NumPy 库函数进行了实验，在 N=1 000，M=280 的网络中，改变分片内节点个数来估算整个区块链分片网络的安全性，并与 RapidChain 分片方案中的网络分片进行对比，如图 4 所示，结果表明本文提出的网络分片方案安全可靠。

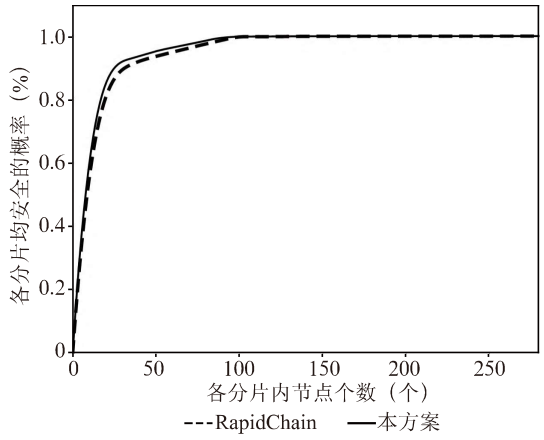


图 4　分片网络安全概率

2.3　扩展性分析

本文方案使用 Python 语言实现并进行了简单模拟。如图 5 所示，将 PBFT 作为共识机制，区块链系统使用分片方案拓展后，交易处理能力得到了提升。

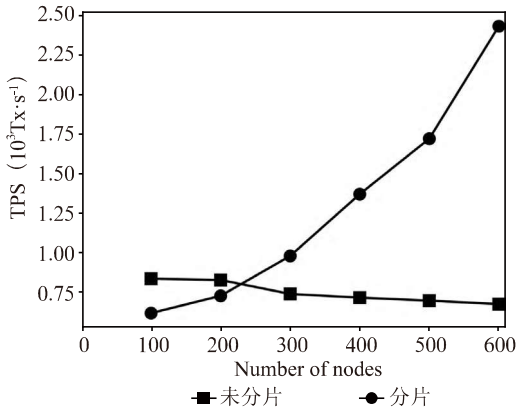


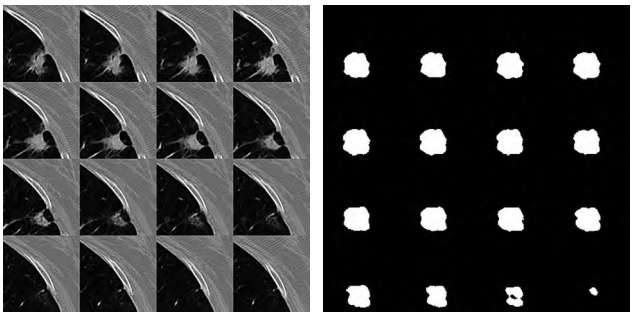
图 5　交易处理能力对比

3　结　论

本文针对区块链系统的交易处理能力不足（下转 35 页）

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

性能的影响，设计出了一种具有分配权重功能的编解码网络 A-Vnet。在 LUNA16 数据集上的实验结果表明，相比于其他算法，A-Vnet 网络的 *F*1- 分数提高了 2%，召回率提高到了 91.4%，较为客观的说明了该模型的精确度。在下一阶段将采用 Transformer 的图像配准方法，用 Transformer 提取全局和局部特征以生成变形场，得到端到端的肺结节分割模型。



（a）原始肺部 CT 图像　　（b）分割结果

图 5　使用 A—Vnet 网络进行肺结节分割的分割效果图

表 2　LUNA16 数据集上不同模型的肺结节分割定量结果

Model	*F*1（%）	Recall（%）
U-Net	66.8	63.48
Attention-Unet	78.7	89.20
V-Net	83.7	81.95
A-Vnet	85.5	91.40

参考文献：

[1] 周清华，范亚光，王颖，等 . 中国肺部结节分类、诊断与治疗指南：2016 年版 [J]. 中国肺癌杂志，2016，19（12）：793—798.

[2] ARMATO S G，GIGER M L，MORAN C J，et al. Computerized detection of pulmonary nodules on CT scans [J]. Radiographics，1999，19（5）：1303-1311.

[3] 魏颖，徐心和，贾同，等 . 基于多尺度形态学滤波的 CT 图像疑似肺结节提取 [J]. 东北大学学报：自然科学版，2008，29（3）：312—315.

[4] 刘慧，张彩明，邓凯，等 . 改进局部自适应的快速 FCM 肺结节分割方法 [J]. 计算机辅助设计与图形学学报，2014，26（10）：1727—1736.

[5] 陈业航，李智，冯宝，等 . 基于改进的活动轮廓模型的胸膜接触型肺结节分割 [J]. 仪器仪表学报，2019，40（11）：107—116.

[6] MILLETARI F，NAVAB N，AHMADI S A. V-Net: Fully Convolutional Neural Networks for Volumetric Medical Image Segmentation [C]//2016 Fourth International Conference on 3D Vision（3DV）.Stanford：IEEE，2016：565-571.

[7] 高慧明 . 基于卷积神经网络的肺结节检测及良恶性分类方法研究 [D]. 太原：太原理工大学，2019.

[8] MNIH V，HEESS N，GRAVES A，et al. Recurrent Models of Visual Attention [J/OL]. arXiv：1406.6247 [cs.LG].[2022-09-18]. https：//arxiv.org/abs/1406.6247v1.

[9] OKTAY O，SCHLEMPER J，FOLGOC L L，et al. Attention U-Net: Learning Where to Look for the Pancreas [J/OL]. arXiv:1804.03999 [cs.CV].[2022-09-18].https://arxiv.org/abs/1804.03999.

[10] 陈铭，梅雪，朱文俊，等 . 一种新型 MobileUnet 网络的肺结节图像分割方法 [J]. 南京工业大学学报：自然科学版，2021，44（1）：76—81+91.

[11] 李传林，黄风华，胡威，等 . 基于 Res＿AttentionUnet 的高分辨率遥感影像建筑物提取方法 [J]. 地球信息科学学报，2021，23（12）：2232—2243.

[12] 门靖茹，王泽荣，张富春，等 . 基于多尺度改进的 V—Net 肺结节分割方法研究 [J]. 延安大学学报：自然科学版，2022，41（1）：115—120.

[13] 高一鸣 . 基于 Gmac 模型的肺结节分割 [D]. 武汉：华中科技大学，2011.

作者简介：刘梦洁（1997—），女，汉族，河南南阳人，硕士研究生在读，研究方向：图像处理。

（上接 31 页） 以媲美中心化应用的问题，提出基于节点属性的分片方案，利用该分片方案对区块链底层进行水平扩容。其中经实验表明提出的节点随机分配方法可使节点随机、均匀地分配到各分片中，并且可验证节点分片结果的正确性；提出交易分片和状态分片方案，降低了跨分片交易的通信开销，降低了区块链系统中节点的存储压力；分析了区块链网络安全性，结果表明扩展后的区块链系统安全可靠；最后对扩展后的区块链系统与传统区块链系统进行了扩展性对比实验。结果表明，基于该分片方案的区块链系统的交易处理能力强于传统的区块链系统的交易处理能力，所以本文提议的基于节点属性分片的区块链系统在满足系统安全的条件下，对区块链系统的交易处理能力有了一定的提升。

参考文献：

[1] 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. Vienna：ACM，2016:17-30.

[2] 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.

[3] WANG J，WANG H. Monoxide：Scale Out Blockchains with Asynchronous Consensus Zones [J].Cryptology and Information Security Series，2019，2019：263.

[4] 秦文慧，李志淮，马洪程 . 状态分片中交易过载处理的节点竞选方案 [J]. 计算机工程与应用，2022，58（22）：89—100.

[5] 刘昌平，刘海 . 一种区块链数据的云存储与共享方法 [J]. 计算机应用研究，2021，38（9）：2600—2603.

作者简介：赵鹏（1973—），男，汉族，山西太原人，教授，博士在读，主要研究方向：软件工程、大数据、区块链；梁晋铭（1996—），男，汉族，山西吕梁人，硕士研究生在读，主要研究方向：区块链技术、共识算法；刘佳宝（1998—），男，汉族，陕西西安人，硕士研究生在读，主要研究方向：区块链共识算法研究。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net