基于 VDF 和一致性哈希的区块链网络分片策略

徐克圣[1] 陈胜男[1] 毛寅辉[1]
XU Kesheng CHEN Shengnan MAO Yinhui

摘 要 分片是一种解决区块链可扩展性问题的关键技术。针对区块链网络分片可能会使恶意节点更容易集中在同一个分片内以及实用拜占庭容错（practical byzantine fault tolerance，PBFT）共识机制主节点选择不合理问题，提出基于可验证延迟函数（verifiable delay function，VDF）和一致性哈希的区块链网络分片方法（blockchain network sharding algorithm based on verifiable delay function and consistent hashing，VCNS）。使用可验证延迟函数随机进行分片，使得恶意节点能够均匀分配到不同的分片中，从而有效避免了大量恶意节点同时控制某个分片的情况，增强了分片区块链的安全性。同时，主节点选举结合一致性哈希算法，由分片内当前主节点选出片内下一个主节点，片内成员节点会验证当前主节点计算出的下一个主节点是否正确，防止当前主节点与恶意节点合谋，增强主节点选举的安全性。实验结果表明，VCNS 在保障分片区块链安全性的前提下，具备了高吞吐量和低共识时延的优势。

关键词 区块链；分片技术；可验证延迟函数；一致性哈希；可扩展性

doi：10.3969/j.issn.1672-9528.2024.04.007

0 引言

区块链是一种基于密码学原理，利用链式区块结构来存储数据的分布式账本技术。区块链以其去中心化、数据不可篡改和公开透明的特点而备受行业关注。然而，目前广泛使用的区块链系统普遍存在可扩展性差的问题，主要表现为系统吞吐量低、交易时延高、存储负担重的情况，这严重限制了区块链技术的发展与应用 [1]。

分片 [2] 是区块链可扩展性技术中最被看好和最受欢迎的技术之一 [3]。该方法的主旨在于将节点分配到不同的区域，让每个区域的节点单独处理不同的交易并各自执行共识，进一步提升吞吐量。虽然分片技术能够明显增强整个区块链系统的交易能力 [4]，但是由于分片会大幅减少各个区域的节点数量，可能会导致恶意节点集中在同一区域进行合谋攻击的情况出现，对整个区块链系统的安全构成威胁。对于保障区块链的安全性而言，如何进行网络分片至关重要 [5]。

目前有许多关于区块链网络分片的研究工作。文献 [6] 通过 PoS 分片协议将交易分割成交易分片，并将网络划分为网络分片。该方法在分片形成后，各片的领导节点需要存储其他分片所有节点的身份信息。一旦泄露了分片信息表，就会引发安全隐患。文献 [7] 基于 PoS 协议采用了公平和动态的分片管理。对于每个纪元，该方法动态地使用 BFT-DPoS 算法并行选择每个分片中的块生产者。该方法每个分片中验证者打包出块的顺序是可预见的，这可能会对区块链的安全造成一定的影响。文献 [8] 采用了分布式哈希表（DHT）随机分片的分片策略，也是基于 PoS 协议的分片方法。该方法是根据计算路由距离进行分片的，不是用于阻止恶意节点同时攻击某一分片的策略。上述基于 PoS 的分片方法并没有实现完全的随机分片，因此某个分片受到攻击的可能性是不可预测的。如果某个分片受到攻击，整个区块链将面临安全风险。

本文提出了一种基于 VDF 的网络分片方法，同 PoW 类似，其使用算力限制恶意节点的加入，不同的是，VDF 可以防止恶意节点并行加速计算。与基于 PoS 的网络分片方法相比，本文的方法降低了女巫攻击和节点聚集攻击的风险，增强了网络分片过程的随机性、公平性和安全性。

为解决 PBFT 主节点选举随意的问题，文献 [9] 采用节点可靠性评分方案来选取主节点并设置共识节点集群来参与共识，减少了共识过程中参与节点的数量，提高了系统效率。文献 [10] 计算节点的有效轮数，再根据其大小选择多个主节点，原 PBFT 算法是选取一个主节点，该方法选取多个主节点进行并发共识，提高了共识的效率。上述研究内容从不同角度解决了 PBFT 算法的问题，但在对选择结果集中化趋势的综合考虑和主节点身份的安全性等方面，改进方案显得更加单一。

1. 大连交通大学软件学院 辽宁大连 116028
[基金项目] 国产化公链基础软件研发与产业化（2022JH2/101300269）

针对 PBFT 共识机制中主节点选择不合理的问题，提出一种基于一致性哈希的主节点选举策略。利用一致性哈希选举主节点，增加了主节点的不可预见性，降低恶意节点被选为主节点的概率，减缓主节点选取集中化的趋势，提高了共识效率和系统稳健性。

1 VCNS 算法设计

1.1 VCNS 的运行过程

在基于 VCNS 的区块链系统中包含了四类节点，分别为最终委员会领导者节点、最终委员会成员节点、分片领导者节点和分片成员节点。为了整个系统的安全，每一个纪元都会重新选取这四类节点。VCNS 在一个纪元中的运行过程如图 1 所示，该系统中所有分片的内部共识都使用 PBFT 共识协议。VCNS 的具体步骤如下：（1）最终委员会领导者生成大量的交易，然后平均分配给分片领导者；（2）在收集到来自最终委员会领导者发来的一定数量的交易后，分片领导者将这些交易打包成一个交易微块，并计算片内打包下一个微块的领导者节点（next_leader），然后把交易微块和 next_leader 的公钥在分片内向成员节点广播；（3）片内节点达成微块共识后，领导者向最终委员会的领导者广播交易微块；（4）最终委员会领导者收集各片的交易微块，并将其组装成交易区块，然后选出委员会中打包下一个交易区块的最终领导者节点（final_next_leader），最终委员会对此区块的结果达成共识后，最终委员会的领导者向分片领导者广播这个新区块，领导者收到后更新区块链状态并向片内其他节点广播区块。同样，片内节点收到该信息后，将该区块更新到区块链。

1.2 网络节点分片策略

为了降低网络分片引起的片内恶意节点合谋攻击风险，本文提出了基于可验证延迟函数的节点分片策略。各节点独立运行可验证延迟函数计算随机数，计算的随机数具有唯一性，使分片结果具有随机性，保证区块链系统的安全。VCNS 节点分片流程图如图 2 所示。VCNS 节点分片过程如下。

（1）初始化阶段

为保证分布式随机生成，确保 VDF 函数去中心化运行，各节点独立计算私钥哈希值，以初始化随机安全参数 λ。通过设置延迟时间 t，使得恶意节点无法利用硬件优势并行加速。最后每个节点运行 *Setup*，生成计算参数 e_k 和验证参数 v_k。*Setup* 函数计算公式为：

$$Setup(sk,t)=(ek,vk) \tag{1}$$

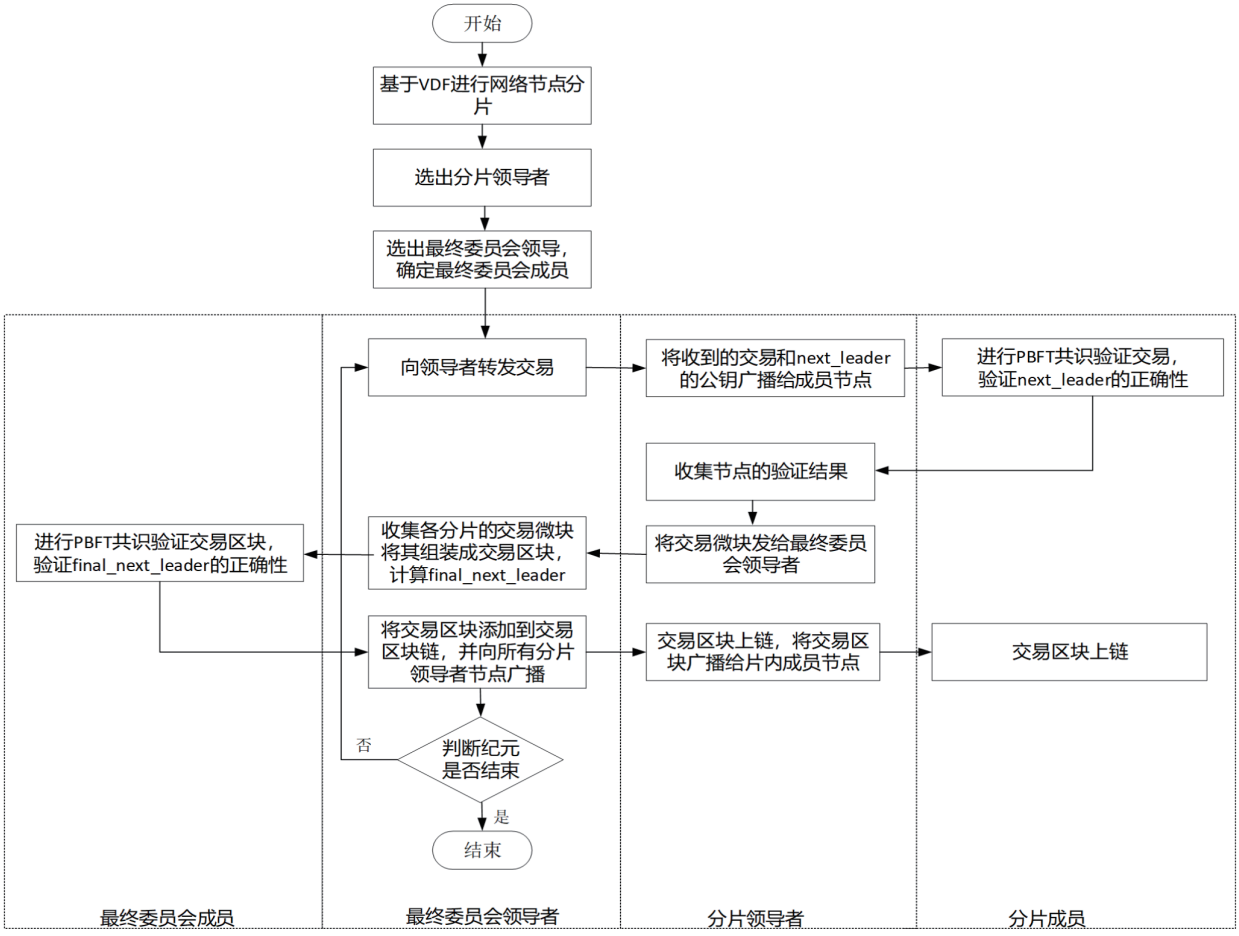


图 1 VCNS 运行流程

（2）计算阶段

各节点在参数初始化完成后，使用公钥哈希值作为输入，运行 VDF 计算函数 *Eval*，广播计算结果 y、证明 π 和验证参数 v_k，以便其他节点进行验证。Eval 函数计算公式为：

$$Eval(ek, pk) = (y, \pi) \quad (2)$$

（3）验证阶段

运行 VDF 验证函数 *Verify*，验证通过将其加入到节点集合中 *nodes.append*(*pk*,*y*)。*Verify* 函数计算公式为：

$$Verify(vk, pk, y, \pi) = (accept \mid reject) \quad (3)$$

（4）分片形成阶段

首先，将节点集合按照 y 值从大到小排序，生成一个 *index* 列表。然后，通过 *index* mod *m*（*m* 为分片个数），得到每个节点的分片号。在每个分片中，第一个大于分片内随机数（y）平均值的节点被选为该分片的领导者。最后，比较所有分片领导者的 y 值大小，y 值最大的领导者所在的分片被选为最终委员会，该领导者则为最终委员会的领导者，该分片的成员即为最终委员会的成员。

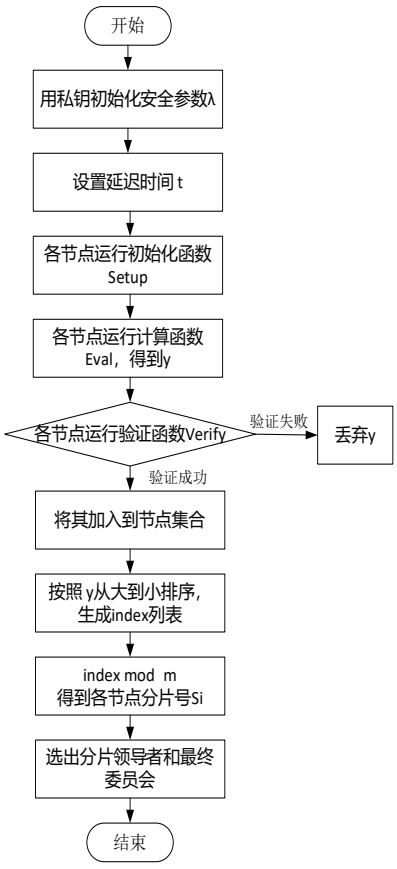


图 2 VCNS 节点分片流程

1.3 领导者选举策略

本方案针对 PBFT 算法中主节点任意选择的问题，提出一种基于一致性哈希算法的分布式主节点选择机制。领导者选举过程如图 3 所示。

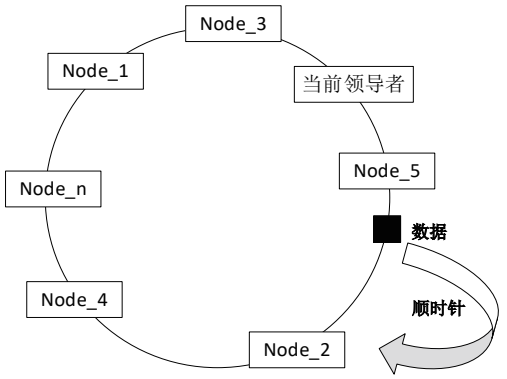


图 3 VCNS 领导者选举过程

领导者选举步骤如下。

（1）一致性哈希算法将哈希值的区域看作一个虚拟的圆环，这些哈希值按照大小顺时针排列。

（2）选择片内各节点的公钥作为关键字用 Hash 函数进行哈希，得到的哈希值映射到圆环上，相当于这些节点处在环上。

（3）分片当前领导者节点将当前微块哈希使用相同的 Hash 函数计算出哈希值，该哈希值也映射到环上，接着再沿着该数据的哈希值进行顺时针寻找，遇到的第一个节点就是片内生成下一个微块的领导者节点（next_leader）。

最终委员会也采用以上方法选出委员会中打包下一个区块的最终领导者节点（final_next_leader）。

1.4 验证主节点策略

分片领导者在生成预准备消息时计算出片内生成下一个微块的领导者（next_leader），并将计算出的 next_leader 的公钥放到预准备消息中，以便在共识阶段片内节点验证 next_leader 的正确性。片内节点收到预准备消息后，会用一致性哈希算法验证当前领导者计算的 next_leader 是否正确，防止当前领导者与恶意节点合谋，增强主节点选举的安全性。片内 PBFT 共识流程如下。

（1）Pre-prepare-npk 阶段：最终委员会领导者将消息请求发送给分片领导者后，分片领导者检验消息的合法性，若验证通过则将预准备消息 <<pre-prepare,V,n,d(m),npk>,m> 发送给片内节点，其中 V 为当前视图编号，n 为序列号，$d(m)$ 为消息 m 的摘要，npk 为当前分片领导者计算出的 next_leader 的公钥。片内节点收到预准备消息后，检验交易是否有效，验证数据和操作的顺序，并且验证当前领导者计算的 next_leader 是否正确，所有信息验证成功的话进入准备阶段。如果节点验证当前领导者计算的 next_leader 不正确，则存在领导节点作恶行为，不再执行下面的共识阶段。

（2）Prepare 阶段：分片内所有成员节点互相发送准备消息 <prepare,V,n,d(m),i>，其中 i 为节点编号。当节点收到超过

2*f*+1 个片内其他成员节点发送的准备消息时，进入确认阶段。

（3）Commit 阶段：分片内各节点包括领导者节点，广播确认消息 <commit,V,n,d(m),i>，当节点收到超过 2*f*+1 个片内其他成员包括领导者节点验证过的确认消息后，消息 m 被执行且变为 committed 状态。

2 实验及分析

本实验使用 Python 语言实现了基于 VCNS 的区块链系统，为了验证 VCNS 算法的可扩展性，将本文提出的 VCNS 算法与 NRSS[11] 和 MACG[12] 分片进行了比较。仿真实验从分片时延、吞吐量、平均共识时延和安全性这四个方面进行对比分析，实验环境如表 1 所示。

表 1 实验环境

对象	配置
CPU	Intel(R) Core(TM) i7-10700 CPU @ 2.90 GHz
操作系统	Ubuntu 20.04
内存	16 GB
软件环境	Python

2.1 分片时延

本文将 VCNS 与基于 PoW 和 PoS 的分片方式进行比较，设置分片个数为 5，节点数从 50 增长至 200，间隔为 25 个节点。结果如图 4 所示。

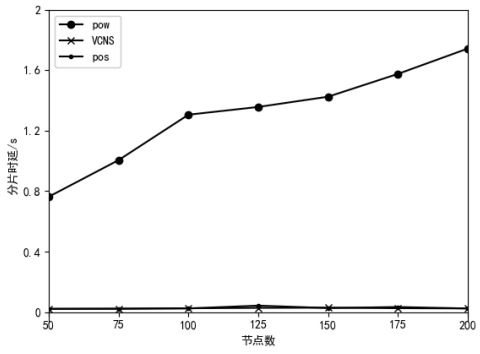
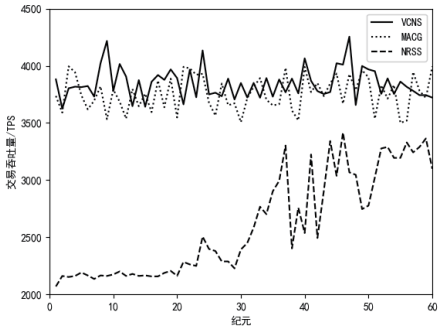


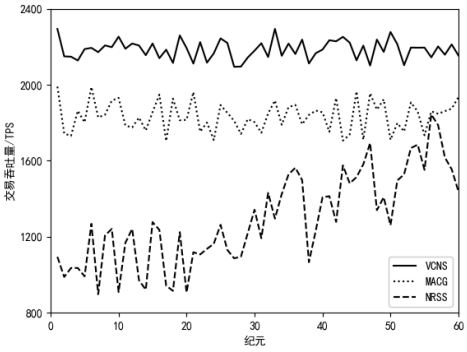
图 4 分片时延对比

2.2 吞吐量

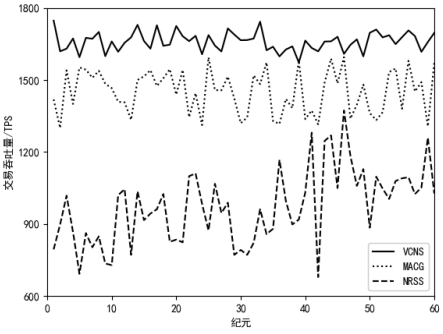
本文通过实验对比 VCNS、NRSS 和 MACG 三者的交易吞吐量。实验设置全网共 1600 个节点，实现三种分片个数的测试，分别为 10 个分片、5 个分片、4 个分片，在分片内节点数为 160、320 和 400 。并且设置每个交易区块中包含 4096 笔交易，最终委员会的领导者会将每个区块中的交易平均分配给所有的分片，并在最后由该领导者组装成交易区块。实验进行了 60 个纪元来测试 TPS 的增长情况，结果如图 5 中（a）、（b）、（c）所示。从 3 个实验结果图可以看出，本方法优于其他两种方案。



（a）分片个数为 10



（b）分片个数为 5



（c）分片个数为 4

图 5 交易吞吐量对比

2.3 平均共识时延

在 VCNS 算法中使用一致性哈希函数来选取主节点，共识过程中若主节点需重新选取，则可能会影响共识时延。

首先测试运行一致性哈希算法所需的时间，设置片内 1000 个节点进行 1000 次实验，测试其运行时间，实验结果如表 2 所示。

表 2 一致性哈希算法运行时间测试

一致性哈希算法	实验次数	总时间 /s	平均时间 /ms
计算出 next_leader	1000	1.899 591 445 922 8	1.899 591

经测试发现，一致性哈希算法的运行时间对 VCNS 算法的共识过程几乎没有影响，当发生视图转换需要使用一致性哈希函数重新选取主节点时，可以忽略其对共识时延的影响。

其次对三种算法的共识时延进行测试，实验设置全网共1600个节点，在将节点分为20个分片、10个分片、5个分片、4个分片的情况下进行测试，同样每个交易区块中包含4096笔交易，进行60个纪元并取共识时延的平均值，结果如图6所示。

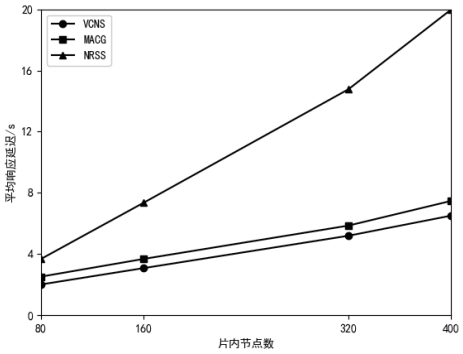


图6 平均共识时延对比

2.4 安全性

测试了当全网节点数为1600时，不同恶意节点比例在不同分片数量下分片失败的概率，如图7所示，当恶意节点数量在网络中所占比例小于四分之一时，VCNS区块链系统的分片方案是安全的。此外，Elastico[13]协议和NRSS同样具有四分之一的最高恶意节点比例，因此VCNS与NRSS和Elastico在安全性方面具有相同的保障。

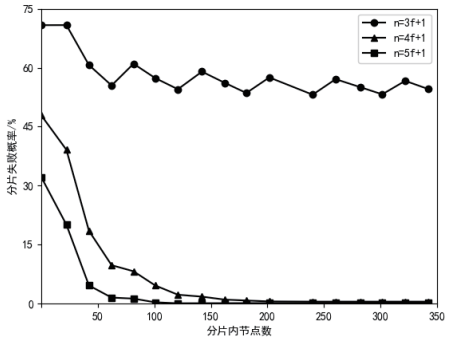


图7 安全性比较

3 结语

基于可验证延迟函数和一致性哈希的区块链分片方法（VCNS）提高了系统的吞吐量和共识效率，VCNS算法的共识过程基于PBFT算法，当系统节点数量过多时，节点间的通信开销会快速增加，从而影响系统的可扩展性。为了解决这一问题，在未来的研究中，应把重点放在让所提到的算法适应更大规模区块链系统的具体研究上。

参考文献：

[1] 孙知信，张鑫，相峰，等. 区块链存储可扩展性研究进展 [J]. 软件学报 ,2021,32(1):1-20.

[2] 黄华威，孔伟，彭肖文，等 . 区块链分片技术综述 [J]. 计算机工程 ,2022,48(6):1-10.

[3]YU G, WANG X, YU K, et al. Survey:sharding in blockchains[J]. IEEE access,2020,8:14155-14181.

[4]LIU Y, LIU J, VAZ S M A, et al. Building blocks of sharding blockchain systems: concepts, approaches, and open problems[J]. Computer science review,2022,46: 10053.

[5] 李皎，王煜田，高耀芃 . 一种抗合谋攻击的区块链网络分片算法 [J]. 计算机应用研究 ,2023,40(1):28-32+41.

[6]GAO Y, KAWAI S, NOBUHARA H. Scalable blockchain protocolbased on proof of stake and sharding [J]. Journal of advanced computational intelligence and intelligent informatics. 2019, 23(5): 856-863

[7]LEE D R, JANG Y, KIM H. Poster: a proof-of-stake (pos) blockchain protocol using fair and dynamic sharding management[C]// The 26th ACM SIGSAC Conference on Computer and Communications Security.New York:ACM, 2019:2553-2555.

[8]DURAND A, ANCEAUME E, LUDINARD R. StakeCube: combining sharding and proof-of-stake to build fork-free secure permissionless distributed ledgers [C]// Networked Systems. Berlin:Springer,2019:148-165.

[9] 唐宏，刘双，酒英豪，等 . 实用拜占庭容错算法的改进研究 [J]. 计算机工程与应用 ,2022,58(9):144-150.

[10] 任秀丽，张雷 . 基于实用拜占庭容错的改进的多主节点共识机制 [J]. 计算机应用 ,2022,42(5):1500-1507.

[11]WANG J, ZHOU Y, LI X, et al. A node rating based sharding scheme for blockchain[C]//2019 IEEE 25th International Conference on Parallel and Distributed Systems,[v.1]. Piscataway: IEEE, 2019: 302-309.

[12] 潘吉飞，黄德才 . 基于跳跃 Hash 和异步共识组的区块链动态分片模型 [J]. 计算机科学 ,2020,47(3):273-280.

[13]LUU L, NARAYANAN V, ZHENG C, et al. A secure sharding protocol for open blockchains[C]//Proceedings of 2016 ACM SIGSAC Conferenceon Computer and Communications Security. New York: ACM, 2016:17-30.

【作者简介】

徐克圣（1965—），通信作者（email:Xks65@126.com），男，辽宁大连人，副教授，研究方向：区块链、软件测试。

陈胜男（1998—），女，辽宁大石桥人，硕士研究生，研究方向：区块链分片技术、机器学习。

毛寅辉（1998—），女，山西朔州人，硕士研究生，研究方向：区块链、自然语言处理。

（收稿日期：2024-01-31）