

Leader Confirmation Replication for Millisecond Consensus in Private Chains

Haiwen Du¹, Dongjie Zhu², Yundong Sun², and Zhaoshuo Tian², *Member, IEEE*

Abstract—The private chain-based Internet-of-Things (IoT) system ensures the security of cross-organizational data sharing. As a widely used consensus model in private chains, the leader-based state-machine replication (SMR) model meets the performance bottleneck in IoT blockchain applications, where nontransactional sensor data are generated on a scale. We analyzed IoT private chain systems and found that the leader maintains too many connections due to high latency and client request frequency, which results in lower consensus performance and efficiency. To meet this challenge, we propose a novel solution for maintaining low request latency and high transactions per second (TPS): replicate nontransactional data by followers and confirm by the leader to achieve nonconflict SMR, rather than all by the leader. Our solution, named leader confirmation replication (LCR), uses the newly proposed future log and confirmation signal to achieve nontransactional data replication on the followers, thereby reducing the leader's network traffic and the request latency of transactional data. In addition, the generation replication strategy is designed to ensure the reliability and consistency of LCR when meeting membership changes. We evaluated LCR with various cluster sizes and network latencies. The experimental results show that in ms-network latency (2–30) environments, the TPS of LCR is 1.4X–1.9X higher than Raft, the transactional data response time is reduced by 40%–60%, and the network traffic is reduced by 20%–30% with acceptable network traffic and CPU cost on the followers. In addition, LCR shows high portability and availability since it does not change the number of leaders or the election process.

Index Terms—Confirmation replication, consensus model, private chain, Raft, state-machine replication (SMR).

I. INTRODUCTION

WITH the introduction of the concept of virtual factories and intelligent manufacturing, the reliability of cross-organizational data sharing has received greater attention [1]. As a valuable data source, the Internet-of-Things (IoT) provides the resources that are required for manufacturing processes, intermediate goods, and manufactured goods.

Manuscript received July 13, 2021; revised August 29, 2021; accepted September 15, 2021. Date of publication September 20, 2021; date of current version May 23, 2022. This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant HIT.NSRIF.201714; in part by the Weihai Science and Technology Development Program under Grant 2016DXGJMS15; and in part by the Key Research and Development Program in Shandong Province under Grant 2017GGX90103. (Corresponding author: Dongjie Zhu.)

Haiwen Du, Yundong Sun, and Zhaoshuo Tian are with the School of Astronautics, Harbin Institute of Technology, Harbin 150001, China.

Dongjie Zhu is with the School of Computer Science and Technology, Harbin Institute of Technology, Weihai 264209, Shandong, China (e-mail: zhudongjie@hit.edu.cn).

Digital Object Identifier 10.1109/IIOT.2021.3113835

These resources are often enriched with sensor, identification, and communication technologies, such as RFID tags [2]. Although many IoT architectures have been generated over the past two decades, they still have problems with trust, security, overhead, and scalability [3].

The public blockchain architecture based on Proof of Stake (PoS) [4] and Proof of Work (PoW) [5] solves trust and security issues well. With good resistance to malicious behaviors, its application in virtual currency has been widely recognized. However, the throughput [lower than 30 transactions per second (TPS)] and confirmation delay (minutes) that they provide cannot meet the demands of IoT systems [6], [7]. To address the problems, direct acyclic graph (DAG)-based approaches represented by Tangle [8] improve the micro-transactions processing performance well. Its confirmation delay depends on the confirmation threshold α and the dependencies of transactions [9]. To build trust between organizations while ensuring high transaction processing efficiency, permissioned private chains use leader-based crash fault tolerant (CFT) consensus protocols (such as Paxos [10] and Raft [11]) and reinforced identification checks [12] to achieve state-machine replication (SMR). Different from Byzantine fault tolerance (BFT) protocols (such as PBFT [13], PoS [4], and PoW [5]), CFT does not allow the existence of Byzantine nodes in the network. Nonetheless, CFT protocols are designed for low-latency distributed systems [14]–[16]. For IoT blockchain systems, sensor data are transmitted using (wireless) sensor networks and are provided through well-defined interfaces, and consensus servers are deployed in wide area network (WAN) environments where the network latency between nodes is unstable [3], [17], [18], as shown in Fig. 1.

As a result, this limitation has several important consequences. First, the massive IoT data lead to data retransmissions when performing SMR due to the high latency, which generates high network traffic between consensus nodes. Second, the centralized SMR incurs worker thread starvation problems on the leader node, which causes a significant decrease in the TPS performance of the blockchain system and increases the high overhead on the leader. Third, followers need to redirect the data to the leader for consistency, which generates additional latency for communicating with a remote leader.

Through research on the data generated by the IoT system, we found that operational nontransactional data are generated at a scale. Different from transactional data, these data contain up-to-date, real-time status information and are less likely to be updated [19]–[21]. Therefore, the availability and timeliness of

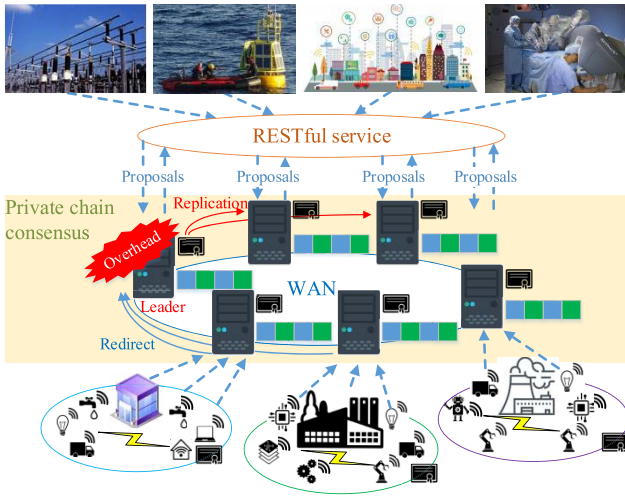


Fig. 1. Architecture of permissioned private chain. In this article, we focus on the optimization of the consistency model to provide better performance and scalability by alleviating the overhead on the leader.

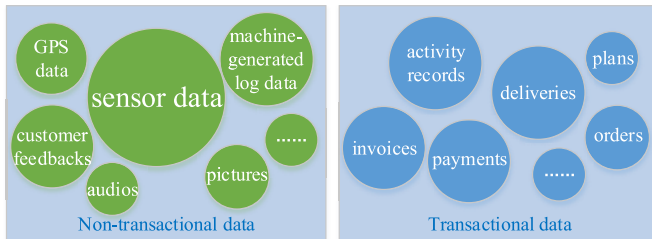


Fig. 2. Examples of transactional and nontransactional data in IoT systems.

nontransactional data are the focus of researchers [22]–[24]. To more clearly distinguish the difference between transactional data and nontransactional data, we give an example in Fig. 2.

Unfortunately, the existing CFT-based IoT blockchain system does not have optimized solutions for nontransactional data, i.e., transactional data and nontransactional data are treated the same. Most existing optimization methods for the geo-distributed consistency are implemented with multi-leader, i.e., the data store is divided into shards with different leaders. Although it can significantly reduce the load of the single leader under high latency, when any node is down, the corresponding shard will be temporarily unavailable due to the re-election. Another type of method dynamically designates leaders [25], but its performance is sensitive to the degree of dependence in the data and is likely to cause inconsistency when the number of nodes is large [26].

We want to reduce the load generated by SMR on the leader in the geo-distributed scenario without damaging the power of the leader and changing the election process, thereby improving the performance of the consistency model. It is common to implement SMR using replicated logs. Therefore, our goal is to make the followers undertake as much nontransactional log replication work as possible. The key point is how the logs replicated by the followers are confirmed by each node to reach a consensus. Among them, it is a challenge to design a novel control method for the leader in the log replication process, which can solve the log replication failure problem

caused by the downtime of the follower nodes [27], [28]. Besides, how to avoid log submission conflicts when followers cannot obtain the entire cluster status in time is also an important problem that we need to solve.

In this article, we propose leader confirm replication (LCR), a method for optimizing leader-based consensus performance in geo-distributed consensus. LCR is the first SMR optimization method that does not change the number of leaders and election strategy and does not add strong control roles to nonleader nodes. It achieves consistency by proposing the future-log, which makes followers become the data leader to replicate the nontransactional data without conflict. The leader only needs to confirm the right replicated future-log by a signal to achieve quorum. In doing so, LCR solves two major problems that we detailed above in geo-distributed scenarios: 1) it decouples the nontransactional data replication process from normal SMR, thereby reducing the leader's resource consumption and improving the consistency efficiency of the data and 2) the entry status information included in each SMR request is increased by applying signal entries and a leader confirmation mechanism. The contributions include the following points.

- 1) We analyzed the cause of the concentrated load problem in the leader-based consistency model and discussed the existing optimization models.
- 2) We designed LCR, detailed the future-log replication model, realized nonconflict log replication, and proved its availability. In addition, we designed generation to resolve log conflicts that can be caused by membership changes in the cluster.
- 3) We implemented LCR based on Raft and compared its performance with popular approaches. Then, we verified its availability and the optimization effect on the request latency, TPS, network traffic, and CPU load in ms-latency network environments.
- 4) We analyzed the overhead of LCR and discussed the application scenarios, which can provide ideas for follow-up studies.

We arranged this article as follows: In Section II, we detail the related work, and in Section III, we show the problems and motivation for the research. We introduce the future-log replication method of LCR in Section IV, and we explain and prove the availability of the model in Section V. In Section VI, we present the experiments that were conducted and the analysis on LCR, and in Section VII, we discuss the protocol. We summarize our work in Section VIII.

II. RELATED WORK

A. Consensus Protocols in Private Blockchains

The rapid development of the private chain technology represented by Hyperledger has made geo-distributed blockchain systems widely used [29]. Different from the public chain, any node needs to go through a reinforced identification check before it can participate in the blockchain network [12]. Therefore, malicious behavior in the private chain will be easily detected and traced. It allows the private chain system

TABLE I
PERFORMANCE COMPARISON OF LCR AND STATE OF THE ART CONSENSUS MODELS

Consistency model	Byzantine Fault Tolerate	Single node overhead	Leader strategy	Client response	Major drawback
PoW[5]	Yes	High	No leader	Tens minutes	High overhead and long confirmation delay
PoS[4]	Yes	High	No leader	Tens seconds	Long confirmation delay
DAG[8]	Yes	High	No leader	Subsecond	High dependence on data business
PBFT[13]	Yes	High	Centralized	3 RTT	Low scalability
Raft[11]	No	High	Centralized	2 RTT	Single point overhead
Multi-Raft[33]	No	Medium	Centralized	2 RTT	Frequent shard leader re-election
Mencius[34]	No	Medium	Rotational	2 RTT	Run at slowest node
Multi-Paxos[35]	No	High	Centralized	2 RTT	Single point overhead
EPaxos [25]	No	Low	No leader	≥ 1 RTT	Higher CPU consumption and more round trips for analyzing dependency
SDPaxos [26]	No	Medium	Centralized	1.5 RTT	More connections between nodes
LCR	No	Low	Centralized	2 RTT (transactional) ≥ 1 RTT (non-transactional)	Our solution

to weaken the security design in an anonymous environment and adopts a consensus model that supports better TPS performance and scalability [30]. Therefore, the existing widely used private chain architectures use CFT protocols (e.g., Raft [11] and Paxos [10]) instead of BFT protocols (e.g., PBFT, PoW, and DAG), thereby improving the cluster scalability and the efficiency of the consistency [14], [31].

However, CFT protocols are designed for low latency environments. In high network latency, most geo-distributed CFT protocols use leader-based SMR to achieve consistency, which can avoid the performance loss caused by replication conflict in the SMR process (e.g., the livelock in Paxos [35]). Nonetheless, the overhead of the leader will cause serious performance degradation when the consistency model runs in high concurrency. Although it is a good idea theoretically to dynamically change the controller of the consensus process to the follower nodes, it requires a stable network environment between each node to obtain the real-time node status. Otherwise, the consistency model will run at the speed of the slowest node [25].

B. Optimization and Application of CFT Protocols in Private Blockchain

As we discussed in Section II-A, the CFT consistency model which is commonly used in private chains, meets leader overhead in geo-distributed environments. To address these issues, existing popular approaches reduce the leader overhead by adopting multiple leaders or reducing the frequency of the log replication times by batching operations. We summarize the consensus models mentioned in this section in Table I.

1) *Leader or Leaderless*: Leaderless consistency protocols represented by Paxos are widely recognized. Researchers have optimized Paxos and proposed some variants to improve its performance in high-latency environments. Since Paxos [10] could have livelock problems in WAN environments, multi-Paxos adds the leader role to it. However, this strategy also places a higher load on the leader node. Mencius [33] makes each node take turns to act as the leader to solve this problem, but this approach makes the performance be determined by

the slowest node. Therefore, EPaxos [25] maintains a leaderless design, which determines the committing method by analyzing the dependencies between operations. If there is no dependency between the operations, then it will use the fast path to reach an agreement. If there is a dependency conflict, an additional round trip is needed to execute ordering constraints to ensure causal consistency. To reduce the extra delay caused by dependency conflicts, SDPaxos [26] adds a sequencer (which can be understood as the leader) to order the data with dependency. Although it reduces the round trip by 0.5, it comes at the cost of a heavier load on the leader and more requests between nodes, which are caused by O -instance. Raft is a simplified version of Paxos. Its single leader strategy requires only one round trip to complete the operation submission. The simplicity of its implementation also makes it widely used in industry and blockchain systems. However, its single-node load problem is an important factor that affects its performance.

2) *Multiple Leaders/Controllers*: To avoid conflicts of control rights, the multileader model divides the data store into multiple shards with different leaders [36], [37]. This method distributes the log replication operation originally led by one node to each node for execution. Although this approach can reduce the overhead generated by the SMR model, making each node act as a leader will make the data replication requests between nodes more frequent. Therefore, TiDB [32] uses connection reuse to ensure that the replication request and response include the metadata of logs and entries, thereby reducing the number of requests between nodes. However, it still cannot solve the frequent leader re-election problem. When any node in the multileader cluster is down, the cluster must invoke re-election; otherwise, the shards that it controls will be unavailable because the node must be the leader of a shard. In addition, during the leader election process, no consensus can be established in the corresponding shards, which will cause availability issues. Therefore, multileader strategy is more suitable for use in a low-latency, high-reliability environment.

3) *Batching Entries*: In addition to multileader, reducing the number of requests in the SMR protocol is another popular

approach to improving the TPS. When the new entries are committed to the leader, using the pipeline to replicate them to the followers is a widely used implementation method of the SMR protocol [38]–[40]. Therefore, researchers designed the buffer to merge the entries and replicate them in one request, which can significantly reduce the SMR requests between nodes, thereby achieving the effect of improving the TPS [41], [42].

However, this approach has two potential problems.

- 1) The average response time will increase. Batching makes the first entry in the buffer wait for subsequent entries to finish writing until the buffer is full, after which the replication method can be invoked by the leader. Nevertheless, it can significantly reduce the replication requests, thereby reducing the load of the leader in high concurrency scenarios. However, when the load is low, the buffer requires a longer time to be fully filled, which will increase the response time [34].
- 2) The followers must keep more connections at the same time. The reason is that the leader must wait for the entries to be applied before returning the success message to the client. Therefore, the followers that forward the client request to the leader must also keep the requests alive. However, this approach will increase the latency, especially in single-ms or higher network latency environments.

III. PROBLEM STATEMENT

The process of SMR between nodes is sensitive to network latency, which easily makes nodes prone to performance problems in geo-distributed systems. Therefore, in this section, we analyze the SMR process in a geo-distributed environment.

A. SMR Performance With Million-Second Latency

Raft numbers the entries and copies them to the follower nodes in order [43]. Thus, Raft can use the *lastIndex* of each node to quickly reach a consensus. However, private chains are widely used in supervised multisubject data-sharing scenarios. The entries they generate contain only a single database operation on new keys. In IoT systems, the leader performs log replication more frequently since the operational nontransactional data are generated on a scale. In addition, the private chain systems need to be deployed in each organization's data center to ensure that they can participate in the consensus [44]. However, we found that the network traffic and I/O overhead generated by the SMR model are very sensitive to network latency. The overhead on the leader will incur higher network overhead and TPS degradation. In addition, most nontransactional requests only insert new key values. The operation of verifying the input and output of the transactions will increase the leader's computing load, resulting in a significant increase in the response time, and adversely affecting the QoS of the private chain system [45].

To better understand the impact of ms-level latency on the efficiency of consistency in geo-distributed systems, we performed experiments on a real-time cross-datacenter backup

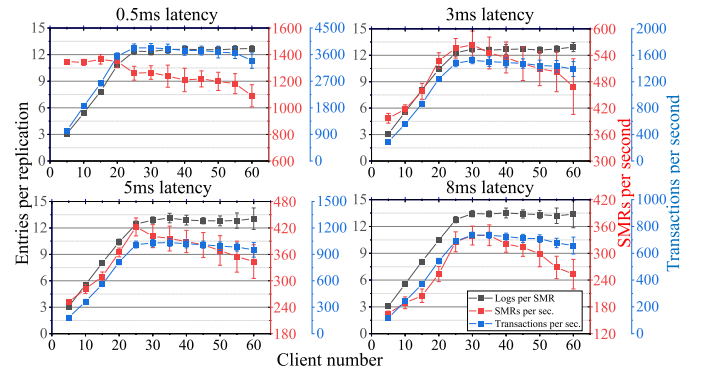


Fig. 3. Different network latencies are added to the 5-node Raft cluster. The x -axis is the number of clients, and the latency fluctuation range and occurrence are 0.1 ms and 30%, respectively. Each request from the client is regarded as a transaction.

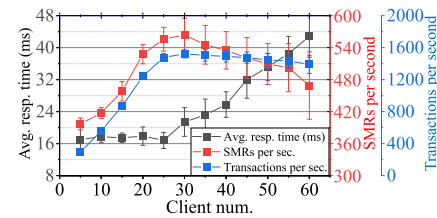


Fig. 4. We conducted a response time experiment under the environment of 3-ms network latency and five nodes. When the number of clients is greater than 25, the average response time gradually increases, and the TPS and replications per sec decrease.

system for Kingsoft Cloud's database, which runs with a 1.5–2 ms network latency, and a Hyperledger-based private chain system, which runs with a 3–7 ms latency. The purpose is to obtain the performance bottleneck of geo-distributed SMR that enables us to make realistic assumptions for the design of LCR-Raft.

In experiments, we send requests concurrently to Raft with numbers of users, and count its TPS and entries' retransmission times under different network latencies, as shown in Fig. 3.

As the number of clients increases, the TPS and the entries per replication of the cluster gradually rise and reach peak performance when the number of clients is less than 25. At this stage, the cluster does not reach its transaction processing capacity, and thus, a stable response time can be guaranteed. With the increase in the number of clients, we observed that the frequency of replication was significantly reduced and the response time increased, as shown in Fig. 4. This outcome occurs because the leader backlogs clients requests or SMR requests due to high network latency, which leads to worker thread starvation or even deadlocks on the leader [46]. Therefore, the limited processing capacity of the leader is a key performance bottleneck of leader-based consistency models in geo-distributed scenarios.

B. Network Traffic Feature of Leader

To express the network load feature of the SMR model more clearly, we took Raft as an example to analyze its log replication process. Ongaro provides the pipeline and

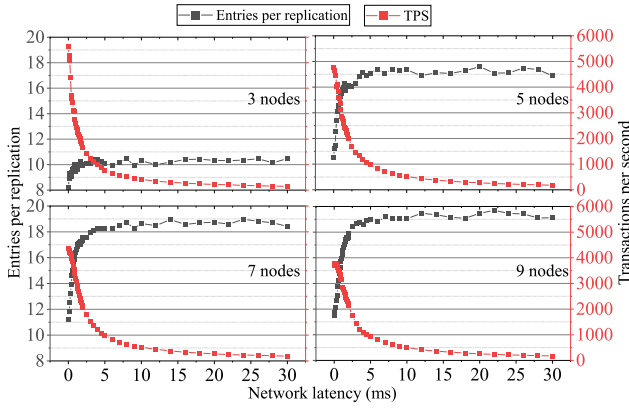


Fig. 5. In the experiment, we added different network latencies to the Raft cluster with 3, 5, 7, and 9 nodes and used a pipeline strategy to replicate entries. The x -axis is the average network latency, and the latency fluctuation range and probability are 0.1 ms and 30%, respectively. It can be seen that as the network latency increases, the entries per replication will increase by 60%–70%.

batching approaches to replicate entries in the initial Raft paper [11], [47]. In practice, there are three main ways to implement it: 1) serial-batching [48]; 2) pipeline [32], [49]; and 3) full parallel [50]. For LAN environments, high routing performance and a stable network are provided. Therefore, it is a better choice to use full parallel or pipeline methods since it can provide a lower response time. However, in geo-distributed systems, network resource are more expensive. In addition, the unstable network environment also makes designers tend to adopt a conservative replication strategy. Accordingly, pipeline strategies were carefully designed by [32] to improve the efficiency of the log replication in geo-distributed scenarios. In an ideal situation, each entry is transmitted $k(n-1)$ times by the leader. However, estimating the round-trip time (RTT) is a key problem for pipeline-based approaches [47] and is not an easy task in WAN environments [51]. For verification, we counted the entry retransmission of the pipeline-based Raft under different network latencies in Fig. 5.

Therefore, it is one of our research motivations to reduce the leader's message transmission cost in the WAN environment.

IV. LOG REPLICATION IN LCR

LCR designed the future-log to distribute the leader's log replication work to followers to alleviate its concentrated load in the consistency model. The future-log can be led by any follower and applied to the state machine using a leader confirmation mechanism. Similar to the log in Raft (we call it normal-log in this article to distinguish it from future-log), future-log is saved as a segmented log on disk and consists of entries and metadata. We call the entries in the future-log future entries and entries in the normal-log normal entries. To make it easier for readers to understand, the figures in this article combine future-log and normal-log, because future entry and normal entry will not conflict on the index in the same node.

Therefore, LCR will not weaken the power of the leader in the replication process. In addition, since the leader uses the confirmation signal to replace the detailed content of the entry,

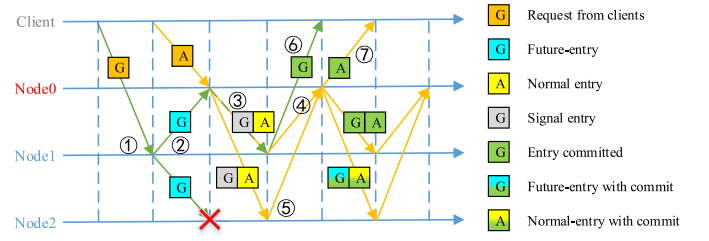


Fig. 6. Data leader will return to the client a success message when it has copied the future-log to most nodes that contain the leader. The future-log will then be confirmed by the leader with a signal and copied to the followers who did not receive the future-log.

TABLE II
DETAILED STEPS OF THE LEADER CONFIRMATION MECHANISM IN FIG. 6

Steps	Operations
1	The follower Node 2 receives the request from the client. Node 2 will create a future entry G, assign a future index to it, and write it to the future log.
2	Node 2 replicates G to other nodes.
3	The leader receives a request from the client, it will create a normal entry A and assign it a normal index. Subsequently, the leader found that entry G in the future-log has not been applied to the normal log, the leader assigns a normal index to it and writes it to the normal log. Then, the leader appends normal entries A and signal entry G to each follower.
4	Node 1 receives the Signal log G, takes the corresponding future entry from the future log according to its future index, replaces the signal log with it, and applies G and A to the normal log. When it is completed, Node 1 responds to the leader that it has applied the index of entry A.
5	Node 2 receives the signal log, but since it cannot find the future entry G in the future log, it will return index-1 of the signal entry G as its lastAppliedIndex to the leader.
6	Node 1 knows that future entry G has been committed, and it will return a success message to the client.
7	The leader learns that more than half of the nodes have applied A; it will commit the entry whose normal index is smaller than A and notify all of the other nodes to commit these entries. Since Node 2 did not successfully apply future entry G, it transmits the raw data of G to Node 2 along with the committed index.

it reduces the leader's network resource consumption. Besides, LCR guarantees that followers have the same standing, which greatly reduces the complexity of the protocol design and makes the membership change process clearer than multileader types of approaches. Here, we detail the leader confirmation mechanism with the messaging model of LCR in Fig. 6 and Table II.

Besides, LCR does not change the leader election attributes. Taking Raft as an example, LCR only needs to add the *futureEntries* property to the request of *AppendEntries* to replicate the future-log between nodes. In the response of *AppendEntries*, the *lastIndex* of the future-log attribute is added, which is used to acknowledge the data leader the max index of the future-log that it has applied, as shown in Fig. 7.

Therefore, LCR is still stateless in the future-log replication process, which makes it possible to maintain a low coupling between the nodes and tolerate unstable network environments.

In this section, we answer the following questions: 1) how the future log is generated and replicated to all nodes; 2) how to resolve the conflict when normal log and future log are allocated the same index; and 3) how to reduce the occurrence of conflicts. Table III collects our notation.

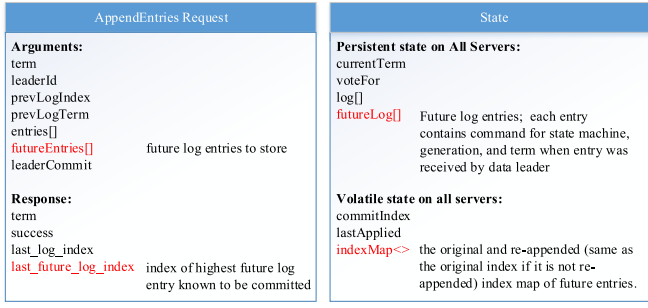


Fig. 7. LCR protocol design. The red attributes are additional in LCR.

TABLE III
NOTATIONS USED IN THIS ARTICLE

Name	Meaning
S_i	a sequenced number that identifies a node.
$lastIndex_i$	the max index of entry that was saved in the segmented log of future-log or normal-log on node S_i .
$nextIndex_i$	the next index that need to be replicated to S_i .
D_t	a transactional data that is generated from a client.
D_{nt}	a non-transactional data that is generated from a client.
G_i	the current <i>generation</i> of node S_i .
E_λ	normal entry with index λ .
FE_λ	future entry with index λ .
Δ_c	the network latency between the cluster and client.
Δ_n	the network latency between the consensus nodes in a cluster.
η	the time period from normal entry packaging to replication request sending on the leader.
η_f	the time period from future entry packaging to replication request sending on followers.
η_w	the time period that a data-leader waits for a signal entry to apply data
ι	the latency that is composed of disk operations latency such as log writing and state machine applying.

A. Future-Log Replication

The numbering method of future entry is similar to the commonly used creasing numbering in the SMR protocol, to make it more applicable to data consistency models. The difference is that the index of two entries that are continuously appended to the future-log can be discontinuous. In addition, the replication process of future-log is led by followers. We call the follower leading a certain future entry replication a data leader and other nodes are data-followers. When a follower with id S_i receives nontransactional data D_{nt} , the follower will become the data leader, allocate a future log index o to D_{nt} , and assemble it into a new future entry FE_λ . The index allocation method is shown in

$$\lambda = S_i + G_i + lastIndex_i - lastIndex_i \% G_i \quad (1)$$

where $lastIndex_i$ is the max index of future entries that S_i saved, and G_i is the current *generation* of S_i (*generation* is an increasing integer as the number of nodes changes and *generation* $\geq \max(S_i)$), which we introduce in detail in Section V).

Theorem 1: The index of future entry FE_λ generated by S_i is globally unique.

Proof: For FE_λ , we can prove that

$$\lambda \% G_i = S_i \quad (2)$$

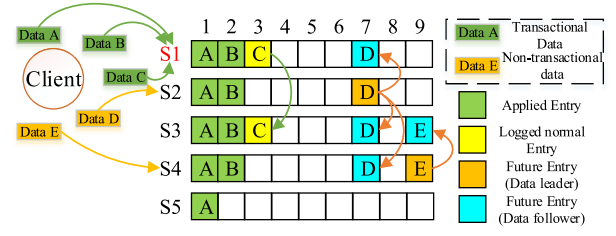


Fig. 8. Example of the future entries replication process, where S1 is the leader.

because

$$G_i \% G_i = 0 \quad (3)$$

$$(lastIndex_i - lastIndex_i \% G_i) \% G_i = 0 \quad (4)$$

and

$$G_i > \max(S_i). \quad (5)$$

Therefore, for servers S_i and S_j , $G_i = G_j$, and the index of future entry that S_i generates must be different from another server S_j .

When $G_i > G_j$, S_i will reject the copy request from S_j . For S_j with an obsoleted G_j , when S_j receives a message from a node with a newer *generation* G_i , S_j can find all of the future entries that it created according to (1). Then, S_j reallocates a nonconflicting index for these future entries with G_i (we will detail how servers address the *generation* change in Section V).

After FE_λ is written on a future-log and committed by the data leader, it copies FE_λ to all nodes, as shown in Fig. 8.

The node will reject the future entry replication request from the nodes with a smaller *term* or *generation* and return the newer information that it knows to them. It ensures that nodes can reach a consensus on the same future entries if and only if the nodes have the same *term* and *generation*. The future entries generated from a node with an obsoleted *term* or *generation* will not be applied because they cannot be accepted by quorum. It is very important because the signal entry must correspond to the same future entry on all nodes. ■

B. Signal Entry and Rereplication

However, the data leader's log replication process could have two problems: 1) the leader receives future entry FE_λ , but parts of the nodes do not receive the FE_λ and 2) the leader did not receive the FE_λ from the data leader.

For the first case, leader S_i does not know which followers have received the FE_λ . Therefore, the leader will use signal entry to replace FE_λ . In particular, if the $nextIndex_j + 1$ of follower S_j is a future entry, FE_j will not be replaced by signal entry. As shown in Fig. 9, S5 did not obtain future entry with FE_7 , and thus, it can only commit a normal entry with E_6 and set $lastIndex_5$ to 6 in the return value. For a follower S_k whose $nextIndex_k + 1$ indexed entry is a future entry, the leader believes that it has not received the future entry $FE_{nextIndex_k+1}$. Therefore, when the leader is packaging entries for replication, it will assemble the entry as a normal entry. Followers will trust the correctness of the leader and commit the entries.

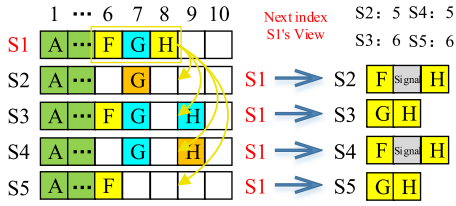


Fig. 9. Example of the signal entry and rereplication process. Since the *nextIndex* of S3 and S5 is 6 and the entry with index 7 is the future entry, S1 believes that S3 and S5 have not received FE₇ (even though S3 has received it).

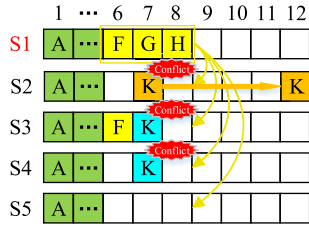


Fig. 10. Example of an entry conflict: each node will unconditionally trust the leader. When a conflict occurs, all nodes except the data leader will discard FE₇, and FE₇ will be reassigned to a new index for the next replication of S2.

For the second case, i.e., when follower S_i with G_i finds that the normal entry E_λ sent by the leader conflicts with FE_λ , the follower trusts the leader. Then, it will check whether the data leader of FE_λ is itself according to

$$\lambda \% G_i == S_i. \quad (6)$$

If the result is *true*, then, S_i is the data leader of FE_λ , and S_i deletes FE_λ from the future-log, reallocates the future entry index according to (1), and rewrite it into the future-log. If it is *false*, it will discard FE_λ . Therefore, regardless of whether the result is *true* or *false*, FE_λ will be written by E_λ , as shown in Fig. 10.

C. Future Entry Index Allocation

We designed a window for LCR to manage the writing process of future entries. A window is a continuous range of index, and it has two states: 1) closed and 2) open. When the window is opened, the node can act as a data leader to write future entries with an index within its window. When the window is closed, the data leader will no longer be able to generate future entries with an index in this range. However, for node S_i , the state of the window does not reject the entries received from other data leaders. The condition for the window to close is that the *lastIndex* of the normal-log (the log that replicated in the sequenced index in SMR) is greater than or equal to the starting index of the window. The window can avoid the conflict described in Section III-B to a certain extent because it can ensure that the allocated index can keep at a distance from the committed index of the leader, as shown in Fig. 11.

In addition, we have added a *generation* property to the window to ensure that there will be no conflict between future entries when the membership changes. We will introduce it in Section V.

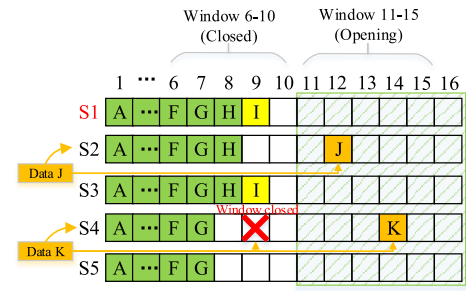


Fig. 11. Example of entry allocation; K will not be written to the position of index 9 because windows 6–10 have been closed when *lastIndex* of S4 is equal to 6.

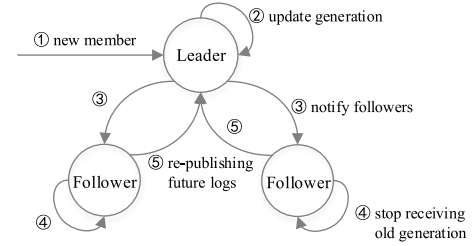


Fig. 12. State transition diagram of *generation*; the numbers represent the trigger sequence.

V. GENERATION FOR MEMBERSHIP CHANGE

In Section IV-A, we mentioned that since the index allocation of the future entries is related to the server id, the dynamic change of the cluster size (membership change) will make the followers meet an index collision. To address the problem, we introduce the *generation*. The *generation* is an integer that contains information about the number of nodes in the cluster. The *generation* and *term* have similar effects. Nodes with higher *generation* will reject future entries' replication requests from nodes with lower *generation*. At the same time, the node will write its *generation* in the request and response. When the *generation* changes, the follower will rereplicate the unapplied future entries that it saves, as shown in Fig. 12.

In this section, we will explain two key concepts of *generation*: 1) the condition that triggers the *generation* change and 2) how to rereplicate the future entries for each node to ensure that the entries can keep consistent after the membership changes.

A. Generation Changing

The *generation* of a node can change under the following three conditions: 1) the node receives the membership changing configuration from the leader; 2) the node learns a newer *generation* from the replication response; and 3) the node learns the new *generation* from the replication request. When the *generation* changes, it will immediately stop sending future entries replication requests and reallocate the index of the future entries that have not been applied to the state machine in such a way that it can be correctly indexed by all nodes. In addition, to facilitate index calculation between nodes, we can use the number of nodes in the cluster as the *generation*. The *generation*'s change rules are flexible. For

example, for clusters that frequently change membership, we can take the surplus of *generation* to reflect the reduction in the number of nodes.

Theorem 2: The increase in *generation* will not cause conflicts between future-logs and normal-logs.

Proof: For node S_i with *generation* G_i , future entry FE_λ and $\lambda \% G_i = S_i$, when the *generation* of S_i becomes G'_i , $G'_i > G_i$, the new index λ' of FE_λ is

$$\lambda' = \left\lfloor \frac{\lambda}{G_i} \right\rfloor * G'_i + S_i. \quad (7)$$

Based on (1), λ' will not duplicate with other future entries in G'_i . In addition, suppose that when the *generation* increases, the leader's *lastIndex* of the normal-log is ω . Then, $\lambda > \omega$ because if $\lambda \leq \omega$, FE_λ must have been committed in the normal-log according to Section IV-B. Here, we prove that $\lambda' \geq \lambda$ and thus prove $\lambda' > \omega$. From (2), we have the following:

$$\lambda = k * G_i + S_i. \quad (8)$$

λ' can be presented as

$$\begin{aligned} \lambda' &= \left\lfloor \frac{\lambda}{G_i} \right\rfloor * G'_i + S_i \\ &= \left\lfloor \frac{k * G_i + S_i}{G_i} \right\rfloor * G'_i + S_i. \end{aligned} \quad (9)$$

Since G_i and G'_i are integers, we have $G'_i \geq G_i + 1$

$$\begin{aligned} \lambda' &\geq \left\lfloor \frac{k * G_i + S_i}{G_i} \right\rfloor * (G_i + 1) + S_i \\ &\geq \frac{k * G_i}{G_i} * (G_i + 1) + S_i \\ &= k * G_i + k + S_i \\ &\geq k * G_i + S_i \\ &= \lambda. \end{aligned} \quad (10)$$

Therefore, the increase in *generation* will not cause FE_λ to conflict with normal entries because λ is larger than any other normal entries. If FE_λ can be applied, then FE_λ must have been successfully replicated to half of the nodes that contain the leader. This circumstance means that FE_λ does not conflict with the normal entries of the leader and thus will not conflict with the normal entries of other nodes, because ω must be greater than or equal to the *lastIndex* of the normal-log of all other nodes. ■

B. Rereplication in Generation Changes

As shown in Section IV, the index allocation method of the future entry is related to the number of nodes. future-log windows with different *generations* cannot keep the same content in future-logs. Therefore, when the node is notified of the *generation* changing, it needs to reallocate and rereplicate the future entries. In detail, when follower S_i obtains the message of *generation* update, it will immediately record all future entries whose index is larger than the *lastIndex* of the normal-log, and clear the windows with the old *generation*. At the same time, it creates a new window with updated *generation*,

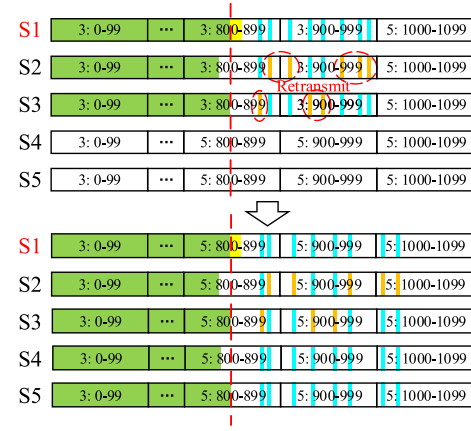


Fig. 13. Example of rereplication in generation changes. The red dashed line is the applied index, and the number format in the box is “generation: window range.” Greens are applied logs; oranges are future entries that are saved in its data leader; blues are future entries that are not saved in its data leader. When generation changes from 3 to 5, each node will reallocate the index for the future entries and rereplicate to other nodes.

reallocates new indexes for these future entries, and starts to replicate the future entries with the new *generation*. Since the *lastIndex* of the normal-log on the follower must be less than or equal to the value on the leader, the follower will not conflict with the entries that have been committed in the normal-log, as shown in Fig. 13.

S1, S2, and S3 store some future entries in two windows: index range 800–899 and *generation* = 3, index range 900–999 and *generation* = 3. When the cluster size changes from 3 to 5, *generation* is also updated to 5. S2 and S3 need to recreate the window with *generation* = 5. In the window where *generation* = 3, the nodes will reallocate the index of future entries in it to the new window according to (1).

Theorem 3: After the *generation* is updated, the rereplication process will not cause inconsistencies in the future-log.

Proof: In node S_i , for an unapplied future entry FE_λ with *generation* G_i , $\lambda \% G_i = S_i$, and *lastIndex* _{i} of the normal-log is ω , $\omega < \lambda$. When *generation* is updated to G'_i , the new index of FE_λ is $\lambda' = \left\lfloor \lambda / G_i \right\rfloor * G'_i + S_i$. In this case, node S_i will replicate FE'_λ to all other nodes with *generation* G'_i . If for node S_j , its *lastIndex* _{j} of the normal-log is greater than or equal to λ' , it will ignore FE'_λ , which also indicates that the leader's *lastIndex* of the normal-log is greater than λ' . Therefore, FE'_λ cannot be applied since it will not be committed by quorum. Node S_i needs to reallocate the index of FE'_λ according to the rereplication strategy in Section IV-B. If for node S_j , its *lastIndex* of normal-log is less than λ' , it will accept FE'_λ on the premise of confirming that its $G_j = G'_i$. According to Theorem 1, the acceptance of FE_λ will not cause conflict. ■

VI. EXPERIMENTS AND ANALYSIS

Due to the complexity of Paxos implementation, Raft has become the main consensus protocol adopted by the private chain due to its advantages in implementation difficulty and efficiency. Therefore, we implemented LCR based on Raft and evaluated it under different network latencies and node

TABLE IV
CONFIGURATION SETTINGS OF THE EXPERIMENTS

Property	Configuration	Comment
election timeout	5000 ms	A follower becomes a candidate if it does not receive any message from the leader in election timeout
max await timeout	1000 ms	The maximum waiting timeout for replicate request.
heartbeat	500 ms	A leader sends RPCs at least this often, even if there is no data to send.
max flying requests	16	Maximum number of concurrent RPC requests.
max entries per request	5000	Maximum number of entries in each RPC request.
max segment file size	100 MB	Maximum number of bytes in each segment.
snapshot period	60 s	Snapshot interval of each node.

numbers to test its scalability and robustness. First, we experiment on the correctness of LCR-Raft to verify its protocol's functional support for native Raft. Second, we evaluate the performance of LCR-Raft to verify its improvement in specific business scenarios. Finally, we compare the optimization effect of LCR-Raft on the leader node in terms of the CPU and network traffic consumption with native Raft and multi-Raft.

A. Environments and Configurations

In order to verify the performance improvement effect of LCR-Raft, we implemented it in the open-source Raft consistency model [50]. Among them, the RPC protocol is implemented using brpc [52], and RocksDB [53] 5.1.4 is used to store state machine data. All of the instances are deployed on 3, 5, 7, and 9 servers (according to the number of nodes in the different experimental configurations) with a Xeon E5-2620 v4 CPU, 64 GB of RAM, 4 TB, and 7200-RPM SATA disk. The system runs CentOS Linux release 7.5.1804, 64 bit, with Linux kernel version 3.10.0. The switch uses H3C Mini S8G-U, with 16-Gb/s switching capacity and 12-Mp/s forwarding performance.

Our client runs on two servers with 6 core 12 thread AMD 3600 CPU and 32-GB memory, and the default number of client jobs is 40. The nontransactional data are the real-time sensor data generated from our blockchain water quality monitoring project, while the transactional data are value transferring operations. The default transactional data and nontransactional data size are 80 bytes. The base configuration of Raft, LCR, and multi-Raft is detailed in Table IV.

It is worthwhile to note that to compare LCR-Raft and other consistency models fairly, we use pipelines to implement SMR, i.e., each log contains only one transaction, and the consensus node immediately invokes remote replication when it generates future entries. The reason is that our work focuses on the optimization of SMR. Although the use of batch messages could improve TPS tens to hundreds of times, its effect is related to the number of clients, the request frequency, the batch size, and the dynamically adjusted request queue, which makes it unable to truly reflect the contributions of our work.

B. Response Time

LCR decouples the replication process of future-log and normal-log. Therefore, for transactional data, the client can still use a normal-log to submit the transactional data. For nontransactional data, using a future-log can significantly reduce

the leader's overhead and the response time of normal entry requests (because normal entries will be processed immediately by the leader). Therefore, in this section, we analyze and test the latency of applying transactional and nontransactional data, and compare it with Raft to verify its optimization effect.

For nontransactional data D_{nt} , the latency Δ_{nt} is

$$\Delta_{nt} = 2\Delta_c + 2\Delta_n + \eta_f + \eta_w + \iota \quad (11)$$

where the Δ_c is the network latency between the cluster and client, Δ_n is the network latency between consensus nodes in the cluster, η_l and η_f are the time periods from entry packaging to replication request sending on the leader and followers, and η_w is the time period during which the data leader wait for a signal entry to apply the data. Here, ι is composed of the disk operation latency, such as log writing and state machine applying.

For transactional data D_t , the latency Δ_t is

$$\Delta_t = 2\Delta_c + 4\Delta_n + \eta_l + \iota. \quad (12)$$

In Δ_{nt} and Δ_t , $2\Delta_c$ is generated from the network latency between client the and nodes. As shown in Fig. 6, it needs $2\Delta_n$ for D_{nt} and $4\Delta_n$ for D_t to respond to the clients.

For Δ_n , since the clients do not know which node is the leader, both transactional data and nontransactional data can be sent to any node. When transactional data are sent to a follower, the follower redirects the request to the leader. In this case, an additional RTT is generated from the redirection. Since this case occurs at a $[(N-1)/N]$ probability, the expected latency is $[(4N-2)/N]\Delta_n \approx 4\Delta_n$. The nontransactional data need $2\Delta_n$ to respond to clients since they will not be redirected. In addition to the Δ_n , the differences in latency for Δ_{nt} and Δ_t are η_w , η_l , and η_f since Δ_c and ι are fixed latencies. From the experiments in Fig. 4, it can be found that the additional latency is generated from η_l (tens-ms) because all other conditions are the same besides the request frequency from the clients. The limited worker threads and high network latency make η_l higher as the client increases. Similar to η_l , η_f increases because the high request frequency of nontransactional data makes followers run under high loads. Here, η_w could be higher than 1 RTT since the leader might not send signal entries to the data-leader immediately when it receives future entries. Besides, the overhead on the leader could amplify η_w . However, η_l will decrease significantly because the proportion of normal entries decreases.

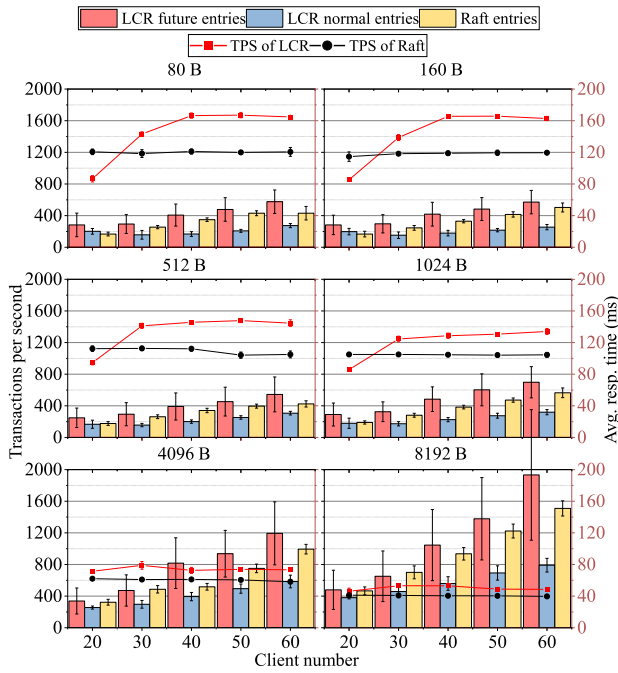


Fig. 14. Comparison between LCR and Raft in TPS and the response time with different request sizes and client numbers.

It allows the leader to reduce the number and frequency of normal entry replication operations. Therefore, the response time of the transactional data in LCR is lower than in Raft.

We tested the effect of LCR and Raft on TPS and the response time in a 5-node, 5-ms latency environment, which is the common network latency between distributed blockchain systems. The proportion of nontransactional (LCR future entries) data was 25%. The result is shown in Fig. 14.

In terms of the TPS, LCR outperforms approximately 30% when the client count is larger than 20. For the response time, as the number of clients and the entry size increase, resource starvation becomes more serious. This circumstance makes the effect of the LCR on reducing the concentrated load more obvious. LCR can provide a 40%–60% response time decrease for transactional data (LCR normal entries), which matches the observation in Fig. 3.

C. LCR Re-Election

To show the availability of LCR, we test the node failures in the cluster. In this experiment, LCR, Raft, and multi-Raft run in a 5-node, 5-ms network latency environment. We randomly stop a nonleader node (an arbitrary node for multi-Raft) at the 10th s and reconnect it to the cluster at the 16th s. In the 25th s, we stop the leader node (an arbitrary node for multi-Raft) and no longer recover it. The result is shown in Fig. 15.

LCR: When the data leader is offline, the future entries that it generates might have not been replicated to all nodes. In this case, the followers that did not receive these future entries will ask the leader to rereplicate these entries, since the leader uses signals to replicate them (as described in Section IV-B). This circumstance will destroy the performance improvement

brought by batching. However, the performance can be quickly restored when these entries are handled. Nonetheless, the TPS will decrease slightly before the node recovers since the downtime of the followers reduces the frequency of future-entry generation, which reduces the optimization effect of LCR. During the 10th s to the 16th s, other followers can still act as data leaders to replicate future entries. Therefore, the performance is not adversely affected (from approximately 1700 to 1600 TPS). When the leader node fails (at the 25th s), it will trigger re-election, which makes the service unavailable during this period. When the new leader is elected (at the 31st s), the TPS performance can recover.

Multi-Raft: In multi-Raft, every node is the leader of shards. For a shard C_i whose leader is S_i , failure on S_i will make C_i unavailable because of re-election. Although the TPS does not drop to 0 (from approximately 1200 to 800 TPS), the remaining TPS is contributed by the active shards. Therefore, the performance of multi-Raft is more sensitive to node failures, since when any node fails, performance fluctuations will occur. However, in LCR and Raft, a nonleader node failure will not lead to serious performance loss. In addition, the availability problem still exists in multi-Raft. Since the probability of each node being offline is the same, the total availability performance is the same as that of Raft.

Raft: Raft suffers the least performance loss when facing a failure of the follower node. However, due to the high load on the leader, its performance under a 5-ms network latency is only approximately 60% (approximately 1200 to 1700 TPS) of the LCR.

D. LCR Performance Experiments

As an important performance indicator of the SMR protocol, we tested the TPS of LCR. In addition, we conducted experiments on the CPU load and network traffic to verify its effectiveness in reducing the load of the leader.

1) TPS: We tested the performance of LCR in terms of the TPS under different cluster sizes and different network latency environments. We designed three clusters with node numbers of 5, 7, and 9. In terms of the network latency setting, we use the *tc* command of Linux to set the simulated delay on the network card and design 41 test points, which are 0, 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1, 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 2, 2.5, 3, 3.5, 4, 4.5, 5, 6, 7, 8, 9, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, and 30. The probability of the network latency fluctuation is 30%, 0.1 ms. We compared LCR-Raft with Raft and multi-Raft. Among them, we optimized multi-Raft using RPC reuse to improve the communication efficiency. On the client side, we created 40 clients to compete to call the RPC protocol to make the cluster work under the maximum load. For LCR, we designed three workloads with different non-transactional data (future entries) ratios, LCR 24%, LCR 40%, and LCR 56% to show the effect of the proportional relationship between the two on the performance of the mechanism. The experiment results are shown in Fig. 16.

To more clearly show the performance of LCR under different network latencies, we divide the performance comparison chart into three intervals (low latency, medium latency, and

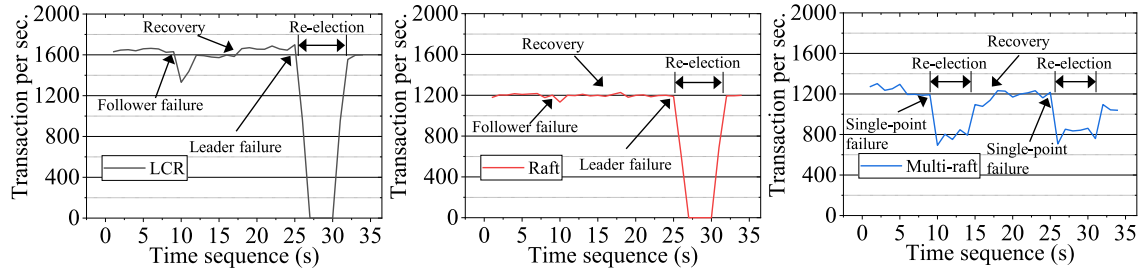


Fig. 15. TPS performance of LCR, Raft, and multi-Raft when facing node failure. The left subfigure is the LCR, the middle subfigure is Raft, and the right side is multi-Raft.

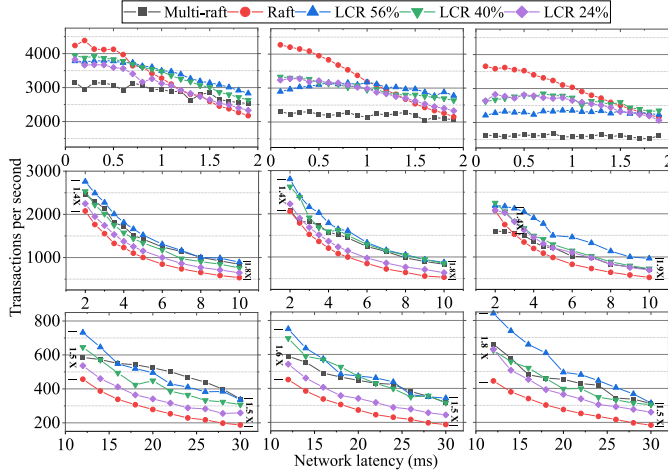


Fig. 16. TPS comparison of LCR, Raft, and multi-Raft in 5, 7, and 9 nodes and different network latency environments.

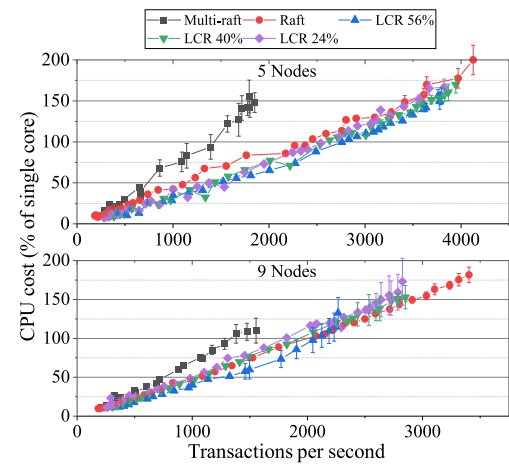


Fig. 17. CPU cost in 5-node and 9-node environments (as a percentage of the single-core max load).

high latency) at 2 and 10 ms. When the network latency is of medium latency and high latency, the LCR has a significant improvement compared with the Raft of approximately 1.4X-1.9X. Under the workload with a higher proportion of future entries, the LCR also has a significant improvement compared to multi-Raft. In the low latency interval, Raft has better TPS performance when the latency is less than 1 ms. Therefore, the effect produced by our model is more suitable for geo-distributed systems with ms-network latency.

2) *CPU Loads*: Since the replication process of the future-log is dominated by followers, it will increase the CPU load on the followers in LCR. Although the leader does not need to control the replication process of future-logs, it still needs to handle signal replacement and retransmission. Therefore, LCR can also generate CPU overhead to the leader. As shown in 6.1, under the same network latency, different consistency protocols have obvious gaps in the TPS. Considering that it is unfair to directly compare the CPU load when the network latency is the same, we use TPS as an x-axis to observe the CPU load of the consistency protocols when they have the same TPS. The experiment results are shown in Fig. 17.

The CPU load of the LCR leader node is similar to that of Raft. When the number of nodes is 5, the CPU load of LCR is slightly higher than that of Raft. When the number of nodes is 9, the CPU load is reduced by 5%–10%.

3) *Network Traffic*: As with the CPU load, we also use TPS as a variable to compare their network traffic. Since LCR

transfers most of the log replication work to followers, when the TPS is the same, the leader node will generate smaller network traffic. Similarly, the degree of network traffic savings is also related to the nontransactional data ratio. Therefore, we computed independent statistics on the LCR traffic under different nontransactional data ratios. The experiment results are shown in Fig. 18.

LCR can save 20%–30% of the network traffic of the leader node. We can conclude that LCR achieves the same TPS as Raft with a lower throughput rate, which can effectively provide saving in the costs of network construction.

E. Overhead Analysis

LCR can generate additional resource costs according to the following three points.

- 1) *Network Traffic*: This cost arises because the follower nodes undertake part of the log replication work. As a result, the network traffic is increased in the followers.
- 2) *Memory Consumption*: The leader needs memory to cache the relational mapping to ensure the writing efficiency of the future-log.
- 3) *Computational Resource Consumption*: Future-log replication requires index calculation and verification. We calculated statistics on these costs to measure whether the extra cost generated by LCR is acceptable.

First, we measure the network traffic. Since additional network traffic is generated on the follower nodes, we will

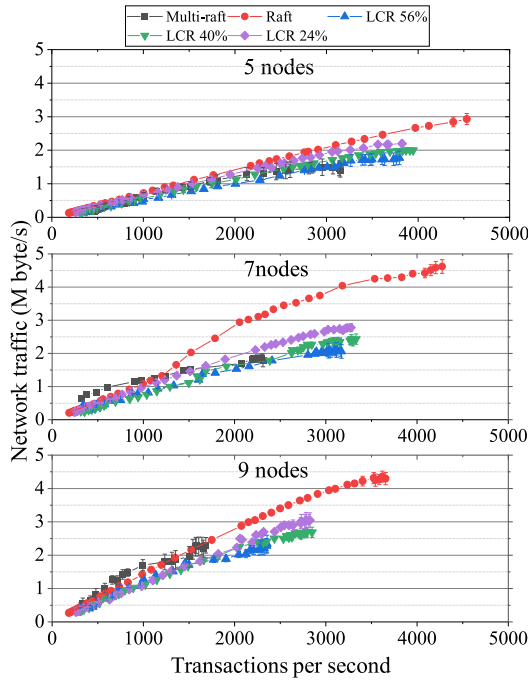


Fig. 18. Comparison figure for the network traffic consumption in a 5-node, 7-node, and 9-node environment.

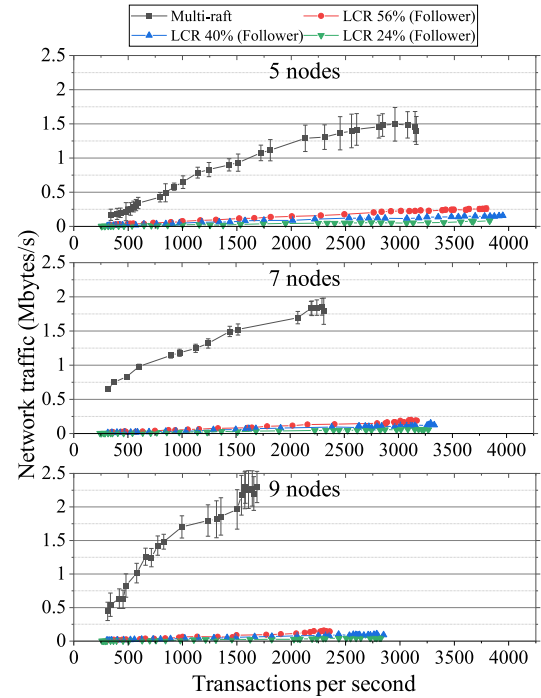


Fig. 19. Additional network traffic from followers.

not compare the leader's network traffic. Here, we count the extra network traffic with different proportions of future entries and compare it with the traffic consumption of multi-Raft. The traffic consumption of multi-Raft is the average of all of the nodes. Similar to Section VI-C, we still compare the traffic consumption under the same TPS. The experiment results are shown in Fig. 19. The additional network traffic generated by LCR is much less than that generated by multi-Raft.

The consumption of the network traffic generated by LCR is much less than that of multi-Raft traffic. At the same time, we found that at the same TPS, the network consumption of the followers will decrease as the cluster size increases. This finding is in line with our expectations because each follower needs to replicate fewer future entries.

In the consistency protocol, the entries must be written to the segmented log and memory at the same time before it is applied to the state machine to ensure that the received log will not be lost. Therefore, future entries need to consume additional memory. We tested the LCR on the extra main memory consumption. The experiments were run in an environment in which the number of consensus nodes is 5, 7, and 9, the average network latency is 5 ms, and the average size of key-value pairs is 80 bytes. The experiment results are shown in Fig. 20.

The experiments show that the consumption of LCR on the main memory is acceptable (KB level) and that the proportion of future entries is positively related to the additional consumption of the main memory. When the number of future entries is too large, the growth rate of its index will far exceed that of normal entries. However, applying the future entries to the state machine must wait for the normal entries whose index is greater than it to be applied. In extreme cases, such as when the proportion of future entries reaches 99%, too many future

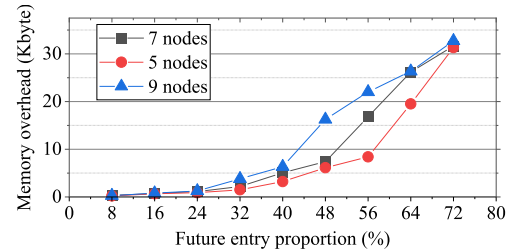


Fig. 20. Additional memory overhead from the nodes in LCR. The experiments run in the 5-, 7-, and 9-node clusters, the average network latency is 5 ms, and the average size of key-value pairs is 80 bytes.

entries will make the growth rate of the normal entries index unable to catch up with the future entries index. This circumstance will cause future entries to wait a very long time before it can be applied. To address this problem, we designed a stepping mechanism to allow the leader to confirm future-entries in advance.

For computational resources, LCR only needs extremely low complexity, such as list and hash map lookup. Although we calculated statistics on leader resource consumption in Section VI-C, our model did not cause a large overhead on the leader node. However, our model will generate an additional CPU load on the follower nodes. We calculate statistics on the CPU load of followers on Raft, multi-Raft, and LCR under different TPSs in a 9-node cluster in Fig. 21.

The results show that the CPU load of LCR will not exceed the leader in Raft. This finding is acceptable since each node should have similar processing capabilities to be elected as the leader. Therefore, the CPU load of LCR will not cause performance degradation.

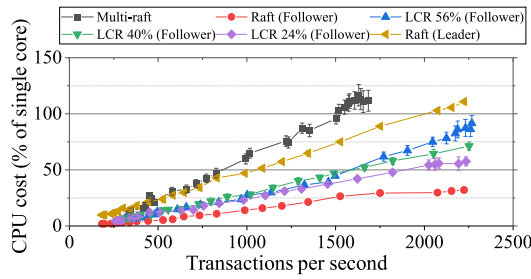


Fig. 21. CPU consumption of nodes with multi-Raft, Raft leader, Raft follower, and LCR.

VII. DISCUSSION

A. Confirmation Versus Multi Leader

LCR is an SMR model based on leader confirmation, but it performs better than semi-synchronous in security. LCR did not decentralize the power of the leader. There is a large number of existing methods that use multileader to reduce the load on the leader, such as multi-Raft [32], Hash Raft [36], etc. However, regardless of the implementation, it will face the following two problems: 1) when any node becomes unavailable, the cluster must invoke re-election and 2) each pair of nodes must synchronize their online status through heartbeats. The leader confirmation method solves these two problems well. First, when the follower node is unavailable, it cannot copy and receive the log from followers and the leader. This circumstance does not require the re-election process. At the same time, compared with multi-Raft, it does not require heartbeats to maintain the online status of each node. Because it does not need the followers to know whether other nodes are online, the follower only needs to know whether the future-logs are accepted by half nodes that contain the leader. Therefore, it does not need to reuse the connection to reduce the network load between nodes, which greatly reduces the complexity of the protocol. In addition, LCR does not guarantee that every future-log has been written into the state machine when it returns a success message to the client. However, it will ensure that data will be written to the state machine at some point in the future, which also makes it applicable to more complex network environments.

B. More Than Raft

LCR is an SMR model based on leader confirmation, but it performs better than semi-synchronous in terms of consistency. LCR did not decentralize the power of the leader. There is a large number of existing methods that use multileader strategies to reduce the concentrated load [32], [36]. However, regardless of the implementation, it will face the following two problems: 1) when any node becomes unavailable, the cluster must invoke re-election and 2) each pair of nodes needs to synchronize their online status through heartbeats. LCR solves these two problems well. For the follower node failure cases, the node cannot copy or receive the log from followers and the leader. It does not require re-election. At the same time, compared with multi-Raft, LCR does not require heartbeats

to maintain the online status of each node. Because followers do not need to know whether other nodes are online, the only thing they care about is whether the future entries are confirmed by the leader, which greatly reduces the complexity of the protocol.

C. Cost

The improvement brought by the LCR does not cause additional costs. As described in Section VI-D, the overhead does not cause consumption that exceeds the original system capacity. Because the log replication process of the SMR protocol is extremely concise, the network, CPU, and other overhead are very sensitive to consensus protocols. As we described in Section II, the increase in the latency will make the TPS drop significantly. To reduce the network latency between geo-distributed nodes, it might be necessary to establish a dedicated network, which is very difficult in terms of feasibility. Although the cost of upgrading the CPU and router is lower, it can also improve the optimization effect brought by the LCR. Therefore, the LCR can trade at a lower cost for the improvement of transactional data consistency efficiency and TPS. In addition, as described in Section VI-C, the LCR can reduce substantially the network traffic. For cluster deployment in WAN, network bandwidth or traffic must be purchased from the Internet service provider (ISP), and the cost is positively related to the bandwidth or traffic. Therefore, the LCR can effectively save approximately 20%–30% of the network construction costs.

VIII. CONCLUSION

In this article, we propose LCR for geo-distributed consensus and nontransactional data. A novel leader confirmation mechanism is proposed, which can reduce the leader's concentrated load. LCR implements a future-log on the SMR protocol and proves its availability. It makes LCR transparent to the election mechanism, which can support various consensus protocols, and combine with other optimization schemes. We implemented LCR based on Raft and tested it in clusters with 3, 5, 7, and 9 nodes. The experimental results show that LCR improves the TPS at 1.4X–1.9X that of Raft, reduces the transactional data response time by 40%–60%, and the network traffic by 20%–30% when the network latency is greater than 1.5 ms compared with Raft. In addition, the overhead on the followers is much lower than that of multi-Raft, and the CPU consumption on the followers is lower than that of the leader node in Raft.

REFERENCES

- [1] S. K. Singh, S. Rathore, and J. H. Park, "BlockIoTelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence," *Future Gener. Comput. Syst.*, vol. 110, pp. 721–743, Sep. 2020.
- [2] S. Schulte, D. Schuller, R. Steinmetz, and S. Abels, "Plug-and-play virtual factories," *IEEE Internet Comput.*, vol. 16, no. 5, pp. 78–82, Sep./Oct. 2012.
- [3] B. Cao *et al.*, "When Internet of Things meets blockchain: Challenges in distributed consensus," *IEEE Netw.*, vol. 33, no. 6, pp. 133–139, Nov./Dec. 2019.
- [4] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proc. Annu. Int. Cryptol. Conf.*, 2017, pp. 357–388.

- [5] S. Nakamoto and A. Bitcoin. (2008). *A Peer-to-Peer Electronic Cash System*. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [6] E. Bandara *et al.*, "Mystiko—Blockchain meets big data," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, 2018, pp. 3024–3032.
- [7] B. Cao *et al.*, "Performance analysis and comparison of POW, POS and DAG based blockchains," *Digit. Commun. Netw.*, vol. 6, no. 4, pp. 480–485, 2020.
- [8] S. Popov, "The tangle," White Paper, 2018. Accessed: Aug. 2021. [Online]. Available: <http://www.descryptions.com/Iota.pdf>
- [9] Y. Li *et al.*, "Direct acyclic graph-based ledger for Internet of Things: Performance and security analysis," *IEEE/ACM Trans. Netw.*, vol. 28, no. 4, pp. 1643–1656, Aug. 2020.
- [10] L. Lamport *et al.*, "Paxos made simple," *ACM SIGACT News*, vol. 32, no. 4, pp. 18–25, 2001.
- [11] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *Proc. {USENIX} Annu. Techn. Conf. ({USENIX}{ATC})*, 2014, pp. 305–319.
- [12] Y. Chen, J. Gu, S. Chen, S. Huang, and X. S. Wang, "A full-spectrum blockchain-as-a-service for business collaboration," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, 2019, pp. 219–223.
- [13] M. Castro *et al.*, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.
- [14] D. Huang, X. Ma, and S. Zhang, "Performance analysis of the RAFT consensus algorithm for private blockchains," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 1, pp. 172–181, Jan. 2020.
- [15] J. C. Corbett *et al.*, "SPANNER: Google's globally distributed database," *ACM Trans. Comput. Syst.*, vol. 31, no. 3, pp. 1–22, 2013.
- [16] M. K. Aguilera, N. Ben-David, R. Guerraoui, V. J. Marathe, A. Xygis, and I. Zablotchi, "Microsecond consensus for microsecond applications," in *Proc. 14th {USENIX} Symp. Oper. Syst. Design Implement. ({OSDI})*, 2020, pp. 599–616.
- [17] X. Zhou, K. Wang, W. Jia, and M. Guo, "Reinforcement learning-based adaptive resource management of differentiated services in geo-distributed data centers," in *Proc. IEEE/ACM 25th Int. Symp. Qual. Service (IWQoS)*, 2017, pp. 1–6.
- [18] J. Hasenburger and D. Bernbach, "GeoBroker: Leveraging geo-contexts for IoT data distribution," *Comput. Commun.*, vol. 151, pp. 473–484, Mar. 2020.
- [19] T. Li, Y. Liu, Y. Tian, S. Shen, and W. Mao, "A storage solution for massive IoT data based on NoSQL," in *Proc. IEEE Int. Conf. Green Comput. Commun.*, 2012, pp. 50–57.
- [20] D. G. Chandra, "BASE analysis of NoSQL database," *Future Gener. Comput. Syst.*, vol. 52, pp. 13–21, Nov. 2015.
- [21] P. Viotti and M. Vukolić, "Consistency in non-transactional distributed storage systems," *ACM Comput. Surveys*, vol. 49, no. 1, pp. 1–34, 2016.
- [22] D. B. Terry, A. J. Demers, K. Petersen, M. J. Spreitzer, M. M. Theimer, and B. B. Welch, "Session guarantees for weakly consistent replicated data," in *Proc. IEEE 3rd Int. Conf. Parallel Distrib. Inf. Syst.*, 1994, pp. 140–149.
- [23] Y. Saito and M. Shapiro, "Optimistic replication," *ACM Comput. Surveys*, vol. 37, no. 1, pp. 42–81, 2005.
- [24] W. Vogels, "Eventually consistent," *Commun. ACM*, vol. 52, no. 1, pp. 40–44, 2009.
- [25] I. Moraru, D. G. Andersen, and M. Kaminsky, "There is more consensus in Egalitarian parliaments," in *Proc. 24th ACM Symp. Oper. Syst. Principles*, 2013, pp. 358–372.
- [26] H. Zhao, Q. Zhang, Z. Yang, M. Wu, and Y. Dai, "SDPaxos: Building efficient semi-decentralized geo-replicated state machines," in *Proc. ACM Symp. Cloud Comput.*, 2018, pp. 68–81.
- [27] A. Ganesan, R. Alagappan, A. Arpaci-Dusseau, and R. Arpaci-Dusseau, "Strong and efficient consistency with consistency-aware durability," in *Proc. 18th {USENIX} Conf. File Storage Technol. ({FAST})*, 2020, pp. 323–337.
- [28] J.-S. Ahn, W.-H. Kang, K. Ren, G. Zhang, and S. Ben-Romdhane, "Designing an efficient replicated log store with consensus protocol," in *Proc. 11th {USENIX} Workshop Hot Topics Cloud Comput. (HotCloud)*, 2019, p. 9.
- [29] M. Muzammal, Q. Qu, and B. Nasrulin, "Renovating blockchain with distributed databases: An open source system," *Future Gener. Comput. Syst.*, vol. 90, pp. 105–117, Jan. 2019.
- [30] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," in *Proc. Int. Workshop Open Probl. Netw. Security*, 2015, pp. 112–125.
- [31] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. IEEE Int. Conf. Syst. Man Cybern. (SMC)*, 2017, pp. 2567–2572.
- [32] D. Huang *et al.*, "TiDB: A RAFT-based HTAP database," *Proc. VLDB Endow.*, vol. 13, no. 12, pp. 3072–3084, 2020.
- [33] C.-S. Barcelona, "Mencius: Building efficient replicated state machines for WANs," in *Proc. 8th USENIX Symp. Oper. Syst. Design Implement. (OSDI)*, 2008, p. 8.
- [34] L. Lamport, "The part-time parliament," *ACM Trans. Comput. Syst.*, vol. 16, no. 2, pp. 277–317, 2019.
- [35] E. Michael, D. Woos, T. Anderson, M. D. Ernst, and Z. Tatlock, "Teaching rigorous distributed systems with efficient model checking," in *Proc. 14th EuroSys Conf.*, 2019, pp. 1–15.
- [36] J. Yang and H. Shen, "Blockchain consensus algorithm design based on consistent hash algorithm," in *Proc. IEEE 20th Int. Conf. Parallel Distrib. Comput. Appl. Technol. (PDCAT)*, 2019, pp. 461–466.
- [37] H. Howard, M. Schwarzkopf, A. Madhavapeddy, and J. Crowcroft, "RAFT refloated: Do we have consensus?" *ACM SIGOPS Oper. Syst. Rev.*, vol. 49, no. 1, pp. 12–21, 2015.
- [38] Z. Zhang, H. Hu, Y. Yu, W. Qian, and K. Shu, "Dependency preserved RAFT for transactions," in *Proc. Int. Conf. Database Syst. Adv. Appl.*, 2020, pp. 228–245.
- [39] B. Carmeli *et al.*, "High throughput reliable message dissemination," in *Proc. ACM Symp. Appl. Comput.*, 2004, pp. 322–327.
- [40] R. Friedman and E. Hadad, "Adaptive batching for replicated servers," in *Proc. 25th IEEE Symp. Rel. Distrib. Syst. (SRDS)*, 2006, pp. 311–320.
- [41] W. Cao *et al.*, "PolarFS: An ultra-low latency and failure resilient distributed file system for shared storage cloud database," *Proc. VLDB Endow.*, vol. 11, no. 12, pp. 1849–1862, 2018.
- [42] D. Wang *et al.*, "Fast log replication in highly available data store," in *Proc. Asia-Pac. Web (APWeb) Web Age Inf. Manag. (WAIM) Joint Conf. Web Big Data*, 2017, pp. 245–259.
- [43] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain technology for cloud storage: A systematic literature review," *ACM Comput. Surveys*, vol. 53, no. 4, pp. 1–32, 2020.
- [44] Y. Yao, X. Chang, J. Mišić, V. B. Mišić, and L. Li, "BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3775–3784, Apr. 2019.
- [45] Y. Zhang, S. Setty, Q. Chen, L. Zhou, and L. Alvisi, "Byzantine ordered consensus without Byzantine oligarchy," in *Proc. 14th {USENIX} Symp. Oper. Syst. Design Implement. ({OSDI})*, 2020, pp. 633–649.
- [46] H. Moniz, J. Leitão, R. J. Dias, J. Gehrke, N. Preguiça, and R. Rodrigues, "BLOTTER: Low latency transactions for geo-replicated storage," in *Proc. 26th Int. Conf. World Wide Web*, 2017, pp. 263–272.
- [47] D. Ongaro, *Consensus: Bridging Theory and Practice*, vol. 1. Stanford, CA, USA: Stanford Univ., 2014.
- [48] *Sofa-Jraft*. Accessed: Nov. 2020. [Online]. Available: <https://github.com/sofastack/sofa-jraft>
- [49] *ETCD RAFT*. Accessed: Oct. 2020. [Online]. Available: <https://github.com/coreos/etcd/tree/master/raft>
- [50] *RAFT-Java*. Accessed: Aug. 2020. [Online]. Available: <https://github.com/wenweihu86/raft-java>
- [51] S. Yasuda and H. Yoshida, "Prediction of round trip delay for wireless networks by a two-state model," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2018, pp. 1–6.
- [52] *BRPC*. Accessed: Oct. 2020. [Online]. Available: <https://github.com/apache/incubator-brpc>
- [53] *RockSDB*. Accessed: Oct. 2020. [Online]. Available: <http://rocksdb.org/>



Haiwen Du is currently pursuing the Ph.D. degree with the School of Astronautics, Harbin Institute of Technology, Harbin, China.

His research interests include distributed storage system architecture and massive data management.



Dongjie Zhu received the Ph.D. degree in computer architecture from Harbin Institute of Technology, Harbin, China, in 2015.

He is an Assistant Professor with the School of Computer Science and Technology, Harbin Institute of Technology, Weihai, China. His research interests include parallel storage systems and social computing.



Zhaoshuo Tian (Member, IEEE) received the Ph.D. degree in physical electronics from the Harbin Institute of Technology, Harbin, China, in 2001.

He is a Professor with the School of Astronautics, Harbin Institute of Technology. His research interests include laser technology and marine laser detection technology.



Yundong Sun is currently pursuing the Ph.D. degree with the School of Astronautics, Harbin Institute of Technology, Harbin, China.

His research interests include social computing and network embedding.