Research on Performance Optimization of Alliance Chain Based on Caching Technology

Xianke Zhou [1], Ziqiang Zhou [2,3], Junlin Zhou [1], Xin Sun [4], Qingyi Huang [1], Shuang Hu [1]

[1] *Institute of Computing Innovation, Zhejiang University, Hangzhou, China, 310008*
[2] *Zhejiang Huayun Clean Energy Co., Ltd. Hangzhou, China, 310008*
[3] *College of Electrical Engineering Zhejiang University，Hangzhou, China, 310027*
[4] *State Grid Zhejiang Electric Power Company Electric Power Research Institute, Hangzhou, China, 310014*

Abstract

Due to its decentralized, tamper proof and traceable characteristics, blockchain has become a research hotspot in academia, and has been applied in government affairs, finance, supply chain, high elastic power grid and other fields. Blockchain technology realizes the safe storage of information and effectively reduces the trust cost of application systems. At the same time, blockchain also has problems such as poor performance and low efficiency, which affect the popularity of applications. In order to solve these problems, this paper proposes a cache optimization method for alliance chain based on the cache of signature information. The experimental results show that after optimization, the transaction delay is significantly shortened, and with the increase in the number of transactions, a relatively stable state can be maintained; The transaction throughput has been increased obviously to improving the performance of the blockchain system.

Keywords

alliance chains; caching technology; Fabric

1. Introduction

In 2008, Satoshi Nakamoto first proposed the concept of blockchain in his paper [1] and used blockchain as the underlying technology to implement the digital currency Bitcoin. After the concept of blockchain was proposed, it has gone through three main development stages [2][3][4]. At present, the development of blockchain technology is in stage 3.0, where blockchain technology starts to combine with industry applications to provide decentralized solutions for different industries and change the application scenarios of many industries with the help of its unique trust mechanism. The application scenarios of blockchain have been expanded to finance, electronic depository, copyright management and trading, product traceability, digital asset trading, supply chain, highly resilient power grid, and many other fields. Olivares-Rojas et al [5] proposed a blockchain-based identity authentication scheme for smart meters to ensure the integrity and validity of transaction data; Tsao Y C et al. [6] proposed a blockchain-based energy trading mechanism to solve a sustainable microgrid design problem.

Blockchain technology has features such as decentralization, de-trust, collective maintenance, reliable database, programmable, and privacy computing [7], and blockchain technology is increasingly used, still facing challenges such as performance issues. Currently, the throughput rate of the system, whether it is a public chain or a alliance chain, still has a large gap compared with traditional software

ISCIPT2022@7th International Conference on Computer and Information Processing Technology, August 5-7, 2022, Shenyang, China
EMAIL: xkzhou@zjuici.com (Xianke Zhou); jx_zzq@sina.com (Ziqiang Zhou); jlzhou@zjuici.com (Junlin Zhou); sun_xin@zj.sgcc.com.cn (Xin Sun); qyhuang@zjuici.com (Qingyi Huang); hs@zjuici.com (Shuang Hu)
ORCID: 0000-0002-4106-7936 (Xianke Zhou); 0000-0001-5191-5321 (Ziqiang Zhou); 0000-0002-0195-7336 (Junlin Zhou); 0000-0002-9115-283X (Xin Sun); 0000-0002-1645-2744 (Qingyi Huang); 0000-0003-0803-7257 (Shuang Hu)

systems. For example, Bitcoin can only process seven transactions per second (TPS), while Ethereum has a throughput rate of over 200 TPS, and Hyperledger Fabric has a throughput rate of over 1000 TPS, which is difficult to meet the needs of industrial-grade application scenarios [8]. The traditional systems Visa and MasterCard can process 1200 to 50000 TPS. The performance issue is the biggest obstacle and challenge for blockchain development. Both academic and corporate communities have made great efforts to improve blockchain performance. Javaid H. et al. [8] analyzed the verification structure of fabric in detail and optimized the structure order of verification by parallelizing verification and database reads, and parallelizing ledger reads and writes with historical data reads and writes, through this scheme it is possible to achieve 1.3 times in the case of LevelDB as a state database throughput and improve the throughput up to 2x with couchDB as the state database. Pissadaki E [9] et al.'s study used lossy compression to reduce the communication cost of sharing state between Fabric backers and verifiers when using blockchain to store intermediate results generated from the analysis of large datasets. Dinh et al. [10] proposed a four-layer software stack and conducted experiments for each layer. The authors also evaluate Fabric using two different workloads and compare Fabric with Ether and Parity.

In this paper, a signature caching optimization approach for alliance chains is proposed to improve the performance.

2. Related Work

2.1 Hyperledger Fabric

Fabric, a component of the open source Hyperledger project hosted by the Linux Foundation, is one of the most active blockchain systems [11]. Fabric's blockchain network uses different types of nodes, such as peer nodes, endorser nodes, sorting nodes, bookkeeping nodes, etc. Peer nodes are the participating subjects in the blockchain decentralized network and are responsible for the execution process of transactions, which are mainly divided into endorser nodes and bookkeeping nodes (Committer) according to their functions, while all peer nodes are responsible for transaction verification and data storage. Endorser nodes are mainly responsible for the pre-execution of transactions in the endorsement stage, and provide endorsement signatures, and endorser nodes are bound to specific chain codes; bookkeeping nodes are responsible for maintaining the state data and ledger, receiving blocks sent from the sorting service, firstly verifying the validity of all transactions inside the blocks, and also verifying whether all transaction endorsements comply with the endorsement policy, and finally writing the blocks into the ledger and updating the state database. The ordering service node, is responsible for sorting the transactions sent from each node and packaging them to generate blocks, thus ensuring data consistency.

The transaction process of Fabric differs from other blockchain systems in that it uses a three-stage execution architecture, i.e., the “endorsement-sort-verify” architecture. In this architecture, nodes are divided into two types of nodes: sequencing nodes and peer nodes [12]. The sorting node is responsible for sorting the transaction, and the peer node is responsible for executing the transaction and maintaining the book data and current state data. The transaction flow is divided into three phases: the endorsement phase, the sorting phase and the verification phase. The details of the transaction are described as follows:

Step 1. The client sends a transaction proposal to the backing node.

Step 2. The endorsing node verifies the signature and simulates the execution of the transaction.

Step 3. The endorsement node sends the endorsement signature to the SDK client.

Step 4. The transaction request is constructed and submitted to the sorting service.

Step 5. The sorting service packs the transactions to generate blocks and distributes them to peer nodes.

Step 6. The transaction is verified and submitted by peer node.

Step 7. Event notification. An event is sent to notify the client that the data has been uploaded and the transaction is valid or invalid.

2.2 Caching Technology

In computer systems, caching techniques are often thought of when transferring data in hardware and software with large differences in read and write speeds. It replaces the medium of relatively low access speed with the medium of high access speed [1].

Caching techniques can be used in the following three roles: (1) performance improvement. The corresponding data will be stored to avoid repeated creation, processing and transmission of data, can effectively improve performance; (2) improve system stability. Caching techniques can reduce the number of accesses to the database, reduce the burden on the database and improve the service capability of the database; (3) improve system availability. The use of caching techniques can improve system availability by providing normal support to end users for a certain period of time in the event of unexpected service stoppages.

3. Signature information caching

From the transaction flow of fabric, the endorsing node will sign the result of the simulated transaction and pack the endorsement signature into the transaction request, which will be verified by the peer node in the transaction verification stage. Usually the endorsing node is also a kind of peer node, that means the endorsing node also performs the verification step of the endorsing signature. This paper proposes a signature caching solution that can effectively improve the blockchain performance.

The execution endorsement phase of the endorsement node is optimized as the following steps as shown in Figure 1.

Step 1. Verify the validity of the transaction, including the integrity of the format, whether it is a duplicate transaction, whether the signature is valid, and whether it has the right to perform the operation.

Step 2. Adding the signature information to the signature global cache of the node if the validation passes; returning an error if the validation fails.

Step 3. Invoking the chain code to simulate the execution of a transaction.

Step 4. Using its own private key to sign the transaction execution result to obtain the endorsement signature.

Step 5. Add the endorsement signature information to the node's signature global cache.

Step 6. Package the endorsement signature information and the transaction execution result into an endorsement response. And then send it to the client.

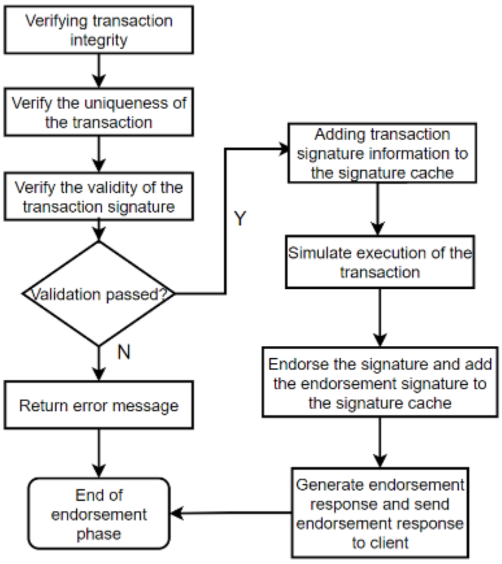
Verifying transaction integrity
Verify the uniqueness of the transaction
Verify the validity of the transaction signature
Validation passed?
Y
N
Return error message
End of endorsement phase
Adding transaction signature information to the signature cache
Simulate execution of the transaction
Endorse the signature and add the endorsement signature to the signature cache
Generate endorsement response and send endorsement response to client

Figure 1 Flowchart of signature cache optimization in endorsement phase

After the peer node receives the blocks packed by the sorting service, it enters the transaction validation phase, which is based on the signature cache optimization process shown in Figure 2, and its main steps are as follows.

Step 1. Verify whether the transaction format is correct.

Step 2. query the cache table to determine whether the transaction signature is in the global cache of the peer node, and if the transaction signature exists, enter step 4.

Step 3. Verify the transaction signature.

Step 4. query the cache table to determine whether the transaction is endorsed by itself, and if it is a transaction endorsed by itself, go to step 6.

Step 5. Verify the endorsement information.

Step 6. Check the version number in the read/write set.

Step 7. Pass the verification, delete the signature cache information, and finish the verification phase.

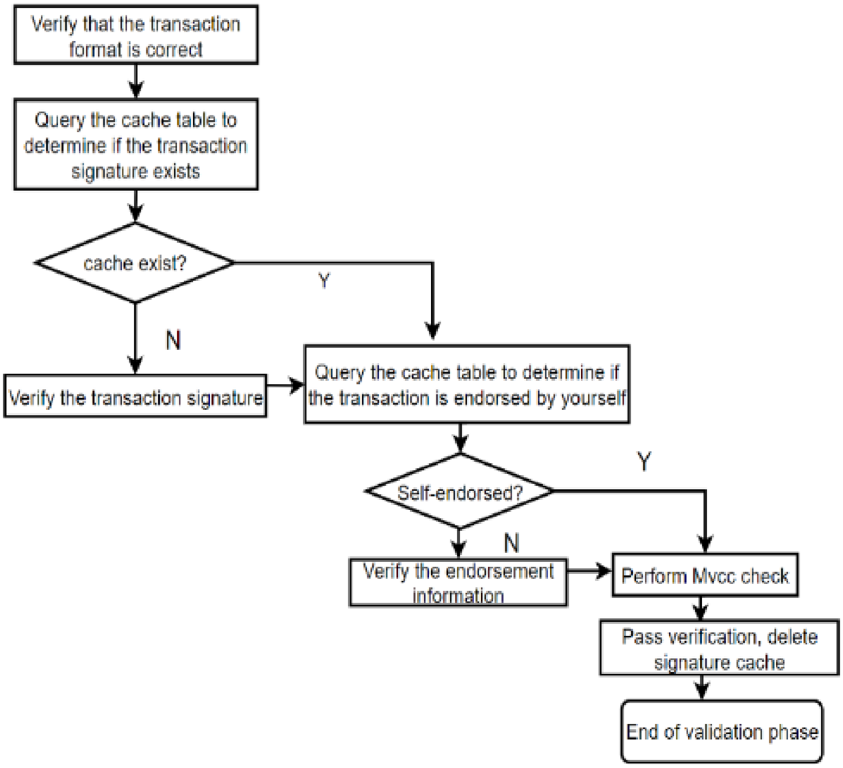
Verify that the transaction format is correct
Query the cache table to determine if the transaction signature exists
cache exist?
Y
N
Verify the transaction signature
Query the cache table to determine if the transaction is endorsed by yourself
Self-endorsed?
Y
N
Verify the endorsement information
Perform Mvcc check
Pass verification, delete signature cache
End of validation phase

Figure 2 Flowchart of signature cache optimization in verification phase

4. Test Analysis

First, the asset transfer contract, which is commonly used in blockchain performance testing, is selected for testing. Then, this section tests the impact of signature cache based on the analysis above. Finally, the performance of the system in comparison with that in the unoptimized state is analyzed and relevant conclusions are drawn.

4.1 Test Environment

This paper chose to use the Hyperledger Caliper tool to better analyze the performance of blockchain networks. Caliper is a blockchain benchmarking framework that allows users to measure the performance of a specific blockchain through a set of predefined of use cases to measure the performance of a particular blockchain. In total, three scenarios are tested, i.e., optimized signature cache, optimized commit cache, and two types of caches. The testing process is divided into two scenarios, namely, optimizing the signature cache, and before optimization state. Table 1 lists the environment configuration information.

Table 1
Test environment configuration information

Projects	deploy
CPU Model	Intel(R) Xeon(R) CPU E5-2620
Number of cores	2
Memory	8GB
Disk Storage	100GB
Operating System	CentOS 7.6
Fabric Version	V1.4
Consensus algorithm	Raft
Number organizations/number of peer nodes in the organization	2/2
Number of sort nodes	4

4.2 Analysis of results

In this paper, the signature caching schemes are tested and analyzed to assess its overall influence to blockchain performance.

Signature caching aims to solve the problem of repeated signature verification by caching signature information and reducing unnecessary signature verification processes, thus improving the performance of the blockchain.

(1) Analysis of transaction response latency

In this paper, we set 100 transactions per block, repeat 10 times, and take the average of 10 tests as the experimental results. The experimental results are shown in Figure 3, where the transaction latency is taken for different total number of transactions. The experiments show that the optimized signature cache can effectively reduce the latency in the same situation, and the latency is also effectively curbed as the number of transactions increases.

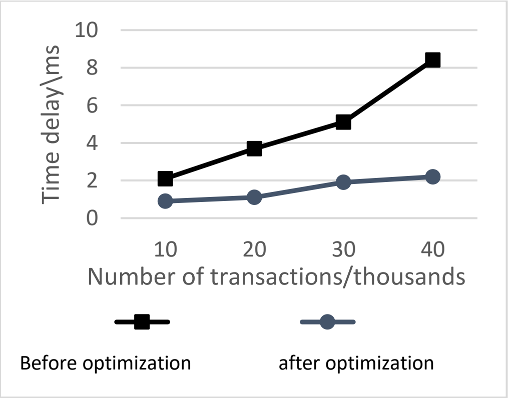

Figure 3 Signature cache optimization latency test chart

（2) Transaction throughput experiment.

As in Experiment 1, 100 transactions per block are repeated 10 times, and the average of the 10 tests is taken as the experimental result. The experimental results are shown in Figure 4 for the throughput situation when taking different total number of tested transactions. The experiments show that the optimized signature cache can effectively improve the throughput of the system and increase the transaction efficiency under the same circumstances.

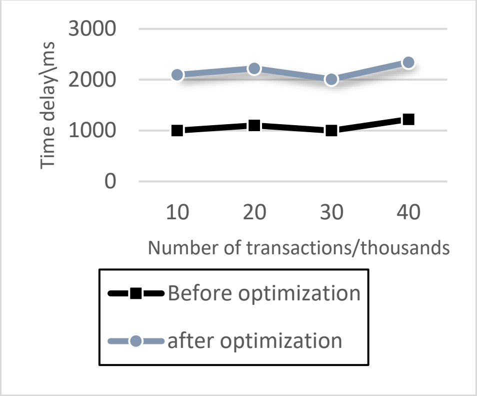

Figure 4 Signature Cache Optimization Throughput Scenario Test Chart

In this paper, we conducted experiments on cache optimization based on Hyperledger Fabric. By caching signature information, we can avoid the problem of repeated signature verification; The experimental results show that the block transaction latency is significantly reduced, the enhancement of the number of transactions does not change the stable line of the system, and the transaction throughput is improved obviously under the same conditions. This indicates that caching technology can effectively improve blockchain system performance.

This work was supported by Science and Technology Foundation of State Grid Zhejiang Electric Power Co. Ltd “research and application of state key technology of blockchain supporting high elastic power grid balance (B311DS21000H)”.

5. references

[1] Nakamoto S. "Bitcoin: A peer-to-peer electronic cash system." Decentralized Business Review (2008): 21260. doi:10.2139/ssrn.3977007.

[2] Wang X, Wang C, Zhou K, et al. "Ess: An efficient storage scheme for improving the scalability of bitcoin network." IEEE Transactions on Network and Service Management (2021). doi: 10.1109/TNSM.2021.3127187.

[3] Wood G. Ethereum: a secure decentralised generalised transaction ledger. Ethereum project yellow paper151.2014 (2014): 1-32. URL: http://gavwood.com/paper.pdf.

[4] Asif M, Aziz Z, Bin Ahmad M, et al. "Blockchain-Based Authentication and Trust Management Mechanism for Smart Cities." Sensors 22.7 (2022): 2604. doi: 10.3390/s22072604.

[5] Olivares-Rojas J C, Reyes-Archundia E, Gutiérrez-Gnecchi J A, et al. "A transactive energy model for smart metering systems using blockchain." CSEE Journal of Power and Energy Systems 7.5 (2021): 943-953. doi: 10.17775/CSEEJPES.2020.05670.

[6] Tsao Y C, VV Thanh. Toward sustainable microgrids with blockchain technology-based peer-to-peer energy trading mechanism: A fuzzy meta-heuristic approach." Renewable and Sustainable Energy Reviews 136 (2021): 110452. doi:10.1016/j.rser.2020.110452.

[7] Kokoris-Kogias E, Jovanovic P, Gasser L, et al. "Omniledger: A secure, scale-out, decentralized ledger via sharding." 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018. doi:10.1109/sp.2018.000-5.

[8] Javaid H, Hu C, Brebner G. "Optimizing validation phase of hyperledger fabric." 2019 IEEE 27th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS). IEEE, 2019. doi:10.1109 /mascots.2019.00038.

[9] Pissadaki E, Varshney K R, Raman R K, et al. Trusted Multi-Party Computation and Verifiable Simulations: A Scalable Blockchain Approach. 2018. doi:10.48550 /arXiv.1809.08438

[10] Dinh T, Wang J, Chen G, et al. BLOCKBENCH: A Framework for Analyzing Private Blockchains. 2017.

[11] Androulaki E, Barger A, Bortnikov V, et al. "Hyperledger fabric: a distributed operating system for permissioned blockchains." Proceedings of the thirteenth EuroSys conference. 2018. doi:10.1145/3190508. 3190538.

[12] Raman R K, Vaculin R, Hind M, et al. "Trusted multi-party computation and verifiable simulations: A scalable blockchain approach." arXiv preprint arXiv:1809.08438 (2018). doi:10.1109/bloc.2019.8751387.