Performance optimization and comparative study of distributed consensus algorithm based on blockchain

Hong A'lan

Software Engineering School, Xiamen University of Technology, Xiamen, 361024, China

Keywords: blockchain; performance optimization; comparative study; distributed consensus algorithm; BFT-DPoSR; PB-RAFT; ER-PBFT; Hybrid-P2P

Abstract: This paper proposes several performance optimization methods, including the improved DPoS algorithm based on node responsibility monitoring (Tower BFT-DPoSR), performance improvements for blockchain systems through hybrid distributed consensus and P2P optimization, the enhanced RAFT algorithm with parallel batch processing (PB-RAFT), and an efficient consensus algorithm involving regional representatives (ER-PBFT). These methods aim to increase transaction processing speed, reduce energy consumption, shorten confirmation time, and enhance the decentralization and security of blockchain systems. Through simulation experiments, this paper compares the performance of Tower BFT-DPoSR algorithm with traditional DPoS, Hybrid-P2P, PB-RAFT and ER-PBFT algorithms in throughput, confirmation time, energy consumption, decentralization degree, security and fault tolerance. The results show that the Tower BFT-DPoSR algorithm has the highest throughput and the lowest energy consumption under all network scales, and has significant advantages in confirmation time. In addition, the algorithm achieves a high degree of decentralization and good fault tolerance through its innovative responsibility evaluation system and hierarchical network model, making it an ideal choice for large-scale and highly concurrent blockchain network scenarios. The research in this paper provides scientific basis and practical guidance for improving the performance of blockchain technology, and lays a solid foundation for building a more efficient, safe and extensible blockchain ecosystem.

1. Introduction

In the wave of digital transformation, blockchain technology has gradually become an important cornerstone to reshape the trust mechanism and promote the development of digital economy with its unique characteristics of decentralization, non-tampering and high transparency. From financial payment, supply chain management to intelligent contract execution, blockchain technology has shown a wide range of application potential, bringing unprecedented opportunities for change to all walks of life. However, with the in-depth application of blockchain, the performance bottleneck of its underlying consensus mechanism has become increasingly prominent, which has become a key factor restricting the large-scale application of blockchain technology [1].

Consensus algorithms, as the core of blockchain technology, are responsible for ensuring all nodes in the network consistently agree on transaction data, serving as the foundation for maintaining the security and reliability of blockchain systems. Currently, mainstream consensus algorithms such as Proof of Work (PoW) and Proof of Stake (PoS) provide decentralized security but also face challenges like slow transaction processing speeds, high energy consumption, and long confirmation times [2-3]. Especially in the face of large-scale transaction processing requirements, these performance bottlenecks not only affect the user experience, but also limit the application potential of blockchain technology in high concurrency scenarios. Therefore, optimizing the performance of blockchain consensus algorithm and exploring a more efficient and environmentally friendly consensus mechanism have become hot and difficult points in the current blockchain research field [4]. By optimizing the consensus algorithm, not only can the transaction processing capacity of the blockchain system be improved and the energy consumption be reduced, but also the decentralization degree and security of the blockchain can be further enhanced, laying a solid foundation for the wide application of blockchain technology.

  DOI: 10.25236/iwmecs.2024.027

This paper discusses the performance optimization method of distributed consensus algorithm in blockchain, and compares the performance of different consensus algorithms. By comprehensively analyzing the advantages and disadvantages of existing consensus algorithms and combining with the latest research results, this paper puts forward targeted optimization strategies. At the same time, through simulation experiments, the performance of traditional consensus algorithm and improved algorithm in throughput, confirmation time, energy consumption and other key performance indicators is compared, which provides scientific basis and practical guidance for improving the performance of blockchain technology.

2. Performance optimization method

2.1. Improved DPoS algorithm based on node responsibility monitoring

To address issues such as unpredictable node behavior, insufficient network security, and limited consensus efficiency in existing Delegated Proof of Stake (DPoS) consensus algorithms, this study proposes an improved algorithm called Tower BFT-DPoSR (Hierarchical Byzantine Fault Tolerance Delegated Proof of Stake with Node Responsibility Monitoring). By introducing a responsibility evaluation system and a group hierarchical network model, the algorithm effectively enhances the fairness and security of the consensus process, significantly reducing the potential threats posed by malicious nodes to the blockchain network [5-6].

The core of Tower BFT-DPoSR algorithm lies in its innovative responsibility evaluation system (see Figure 1). The system assigns a dynamic responsibility score to each node by comprehensively considering the historical behavior, voting integrity, online time and enthusiasm for participating in consensus. This score not only reflects the reliability and contribution of nodes, but also serves as an important reference for nodes to participate in the consensus process.

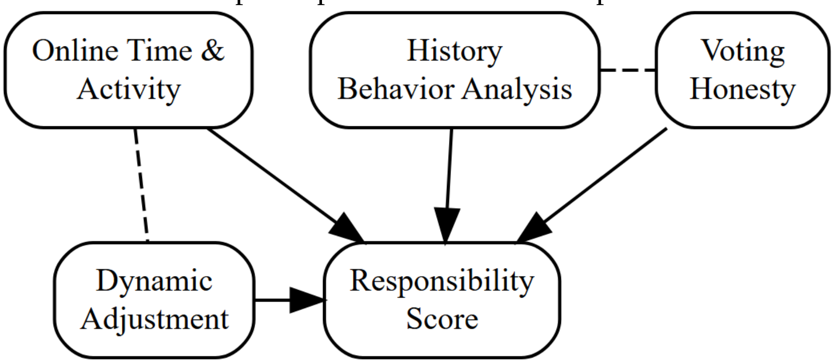

Figure 1 Responsibility evaluation system

By tracking the transaction records and voting behavior of nodes through the tamper-proof characteristics of blockchain, its integrity is evaluated; At the same time, according to the performance of the node in the election process, it is judged whether it abides by the community rules and whether it has malicious voting or brushing votes. Then, combined with the online time of nodes, the frequency of participating in consensus and the response speed, the enthusiasm of their network participation is comprehensively evaluated; Finally, the node's responsibility score will be dynamically adjusted according to its real-time behavior to ensure the fairness and timeliness of the evaluation system.

In order to further improve consensus efficiency and reduce communication overhead, Tower BFT-DPoSR adopts a packet layered network model, as shown in Figure 2. In this model, the nodes in the network are layered according to the responsibility score, and organized into multiple groups according to the hierarchical relationship. After the local consensus is reached within each group, the group opinions are formed, and then the overall consensus is reached by the representatives of each group, and finally the whole network is consistent.

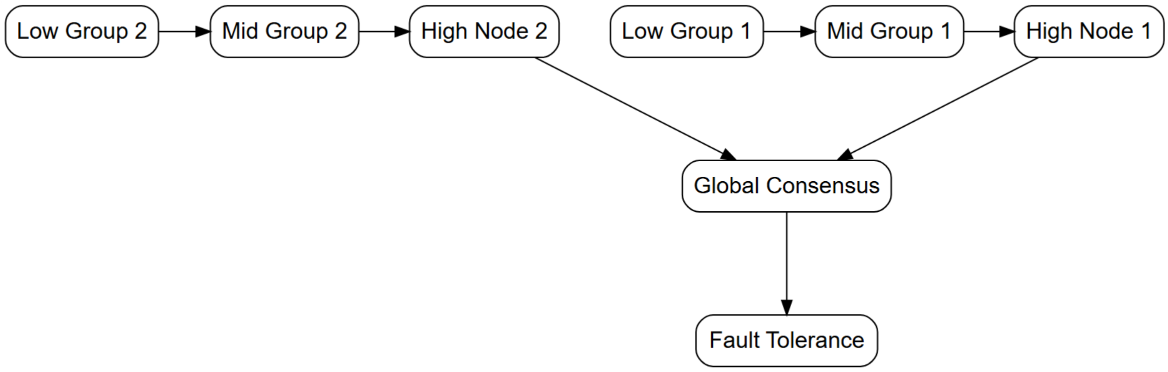

Figure 2 Packet layered network model

According to the responsibility score, the nodes are layered, and the nodes with high scores enjoy higher trust and decision-making power; Nodes in the same level are subdivided into multiple groups, and an efficient consensus algorithm (such as PBFT) is used to quickly reach group consensus. Subsequently, the representatives of each group submit the consensus results to higher-level nodes to achieve global consensus and ensure the consistency of the whole network; Through redundant design and Byzantine fault-tolerant algorithm, the whole system can maintain the accuracy of consensus and the security and stability of the network even if there is node failure or malicious behavior.

Through the combination of responsibility evaluation system and grouping hierarchical network model, Tower BFT-DPoSR algorithm significantly improves the fairness and security of consensus process. The responsibility evaluation system ensures that only the nodes with high integrity and great contribution can obtain higher decision-making power, which effectively prevents the interference and destruction of malicious nodes. At the same time, by combining local consensus and global consensus, the hierarchical network model reduces the communication overhead and improves the consensus efficiency, so that the blockchain network can handle large-scale transactions more efficiently.

2.2. Other optimization methods

The rapid development of blockchain technology has placed higher demands on the performance of consensus algorithms. To address challenges such as slow transaction processing speeds, long confirmation times, and high energy consumption, researchers are continuously exploring new consensus algorithms or optimizing existing ones. This paper introduces several innovative performance optimization methods, including performance improvements for blockchain systems through hybrid distributed consensus and P2P optimization, the enhanced RAFT algorithm with parallel batch processing (PB-RAFT), and an efficient consensus algorithm involving regional representatives (ER-PBFT).

(1) Performance improvement of blockchain system based on hybrid distributed consensus and P2P optimization

Hybrid distributed consensus combines the advantages of various consensus algorithms to meet the needs of different scenarios [7]. For example, a lightweight consensus algorithm can be used to improve efficiency when the network load is low, and a more robust algorithm can be switched when the network load is high or the security requirements are higher. In addition, by optimizing the P2P network layer, the speed and reliability of message propagation can be further improved, and the delay in the consensus process can be reduced.

The key optimization points include the dynamic consensus mechanism of dynamically selecting the optimal consensus algorithm according to the network conditions; P2P network optimization can improve the efficiency of message propagation and reduce the delay and packet loss rate through layered P2P network and multi-level broadcasting. And cross-chain communication technology that realizes efficient communication between different blockchains and supports cross-chain transactions and asset transfer.

(2) PB-RAFT algorithm

PB-RAFT optimizes the traditional RAFT algorithm [8]. Through parallel processing, batch processing and pipeline technology, the parallelism of log copying and status updating operations, the packaging of multiple requests to reduce communication overhead and context switching costs, and the overall throughput are improved by optimizing the processing flow, thus significantly improving the performance of RAFT algorithm in large-scale distributed systems.

(3) ER-PBFT algorithm

ER-PBFT is an efficient consensus algorithm designed for large-scale distributed networks. Based on PBFT algorithm, it reduces the communication complexity and improves the efficiency by setting up a regional representative mechanism [9]. The key optimization point is that the network is divided into multiple regions, and each region selects representatives to participate in the global consensus, which effectively reduces the number of nodes directly participating in the consensus and reduces the communication cost. The lightweight consensus algorithm is used to achieve local consensus in the region, and then the regional representatives complete the global consensus, which further improves the efficiency; In addition, the algorithm also enhances the fault-tolerant ability, and ensures that the consensus can still be reached correctly in the presence of malicious or faulty nodes.

Through the above performance optimization method, the performance of blockchain consensus algorithm can be significantly improved to meet the needs of different scenarios. The method based on hybrid distributed consensus and P2P optimization improves the flexibility and scalability of the system. PB-RAFT improves the processing efficiency through parallel batch processing; ER-PBFT reduces communication complexity and improves consensus efficiency through regional representation mechanism. These optimization methods not only provide strong support for the development of blockchain technology, but also lay a solid foundation for building a more efficient, safe and extensible blockchain ecosystem.

3. Performance comparison of consensus algorithm

In order to evaluate the performance of Tower BFT-DPoSR algorithm, this paper compares it from five dimensions: throughput, confirmation time, energy consumption, decentralization degree, security and fault tolerance. These indicators respectively measure the transaction processing ability, transaction confirmation speed, energy consumption, node distribution and decision-making power dispersion, and the ability to resist malicious attacks and failures of blockchain system.

In the simulated network environment, blockchain networks of different scales are simulated by changing the number of nodes (from tens to thousands), so as to compare the performance of Tower BFT-DPoSR algorithm with DPoS, Hybrid-P2P, PB-RAFT and ER-PBFT algorithm in key performance indicators such as throughput, confirmation time and energy consumption. The experiment uses a specially developed test framework to measure these indicators, and sends a large number of transactions to the network through a simulated transaction generator, and repeats the experiment many times to ensure the stability and reliability of the data.

Figure 3 shows the throughput comparison of different consensus algorithms under different network scales. As can be seen from the figure, Tower BFT-DPoSR algorithm shows the highest throughput in all network scales, especially in large networks. PB-RAFT and ER-PBFT also show higher throughput, but slightly lower than Tower BFT-DPoSR. However, the throughput of DPoS and Hybrid-P2P is relatively low, especially when the network scale increases, the performance decline is more obvious.

Tower BFT-DPoSR algorithm shows the most efficient transaction processing ability with a confirmation time of about 2.5s, which is especially suitable for application scenarios with high speed requirements; The confirmation time of PB-RAFT and ER-PBFT is 3.2s and 4.1s, respectively, which is slightly lower than that of Tower BFT-DPoSR, but it remains at a low level and performs well. In contrast, the confirmation time of DPoS and Hybrid-P2P is longer, 5.6s and 6.8s respectively, which may affect the user experience in large-scale network or high transaction volume environment. Overall, Tower BFT-DPoSR has obvious advantages in confirmation time, while PB-RAFT and ER-PBFT are also good choices, while DPoS and Hybrid-P2P are slightly insufficient in confirmation time. The comparison of confirmation time of different consensus algorithms is shown in Figure 4.

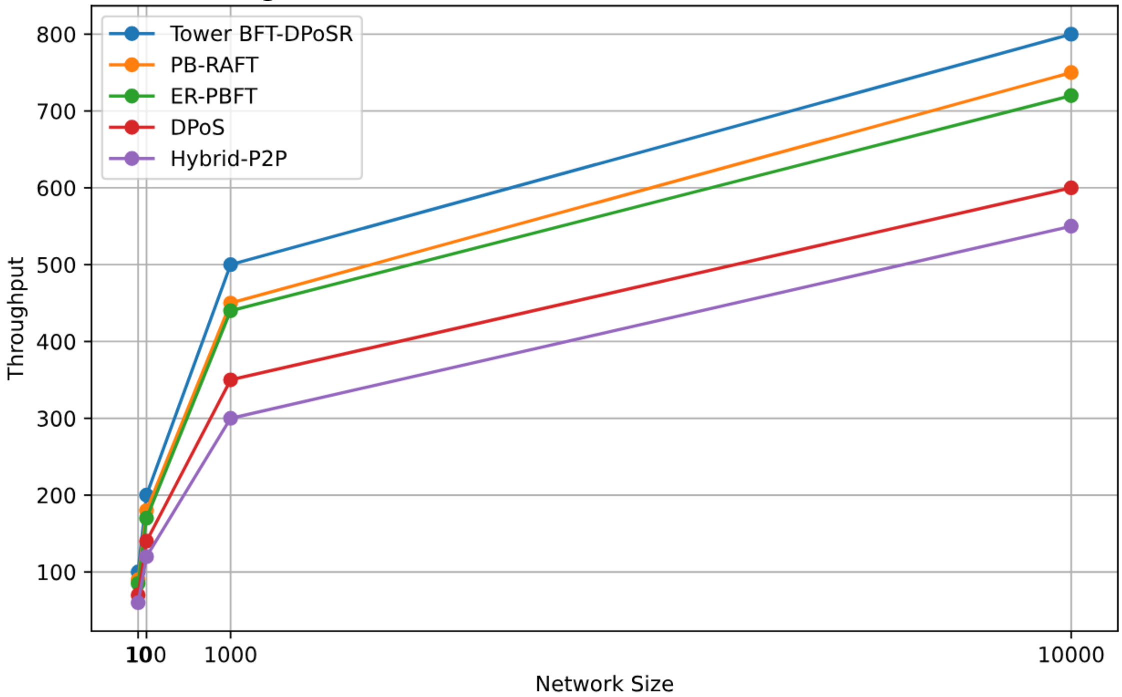

Figure 3 Throughput changes of different algorithms under different network scales

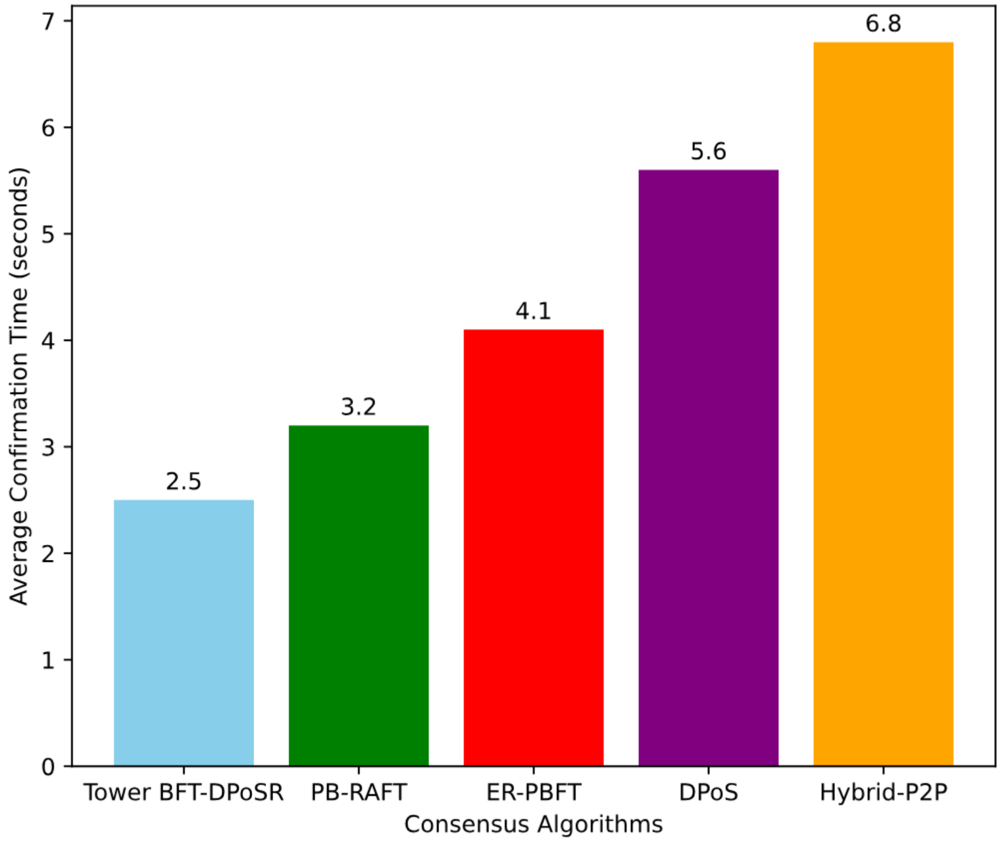

Figure 4 Confirmation time of different consensus algorithms

Table 1 shows the differences of energy consumption among the algorithms, among which Tower BFT-DPoSR stands out with the lowest energy consumption of 12.3 kJ, thanks to its optimized consensus process and efficient communication mechanism. The energy consumption of PB-RAFT and ER-PBFT is 17.8 kJ and 20.5 kJ respectively, which is higher than that of Tower BFT-DPoSR, but still at a low level. However, the energy consumption of DPoS and Hybrid-P2P increased significantly, reaching 29.6 kJ and 32.4 kJ respectively, which indicates that they consume a lot of energy when dealing with large-scale networks or high transaction volume, which is not conducive to long-term sustainable operation.

Table 1 Energy consumption of different consensus algorithms in the network

Consensus algorithm	Energy consumption (kJ)
Tower BFT-DPoSR	12.3
PB-RAFT	17.8
ER-PBFT	20.5
DPoS	29.6
Hybrid-P2P	32.4

Tower BFT-DPoSR has achieved a high degree of decentralization and security through the grouping hierarchical network model and responsibility evaluation system, and can maintain correct consensus and network security even if some nodes are malicious or fail; ER-PBFT also achieves high decentralization and good fault tolerance through regional representation mechanism; However, DPoS and Hybrid-P2P are relatively weak in decentralization and security because they rely on elected representatives. The degree of decentralization and security of PB-RAFT depends on the specific deployment mode, but it usually needs the coordination of leading nodes, which may affect its decentralization level.

To sum up, Tower BFT-DPoSR algorithm shows excellent performance in throughput, confirmation time, energy consumption, decentralization degree, security and fault tolerance. Compared with traditional DPoS algorithm and other optimization algorithms, Tower BFT-DPoSR is more suitable for large-scale and highly concurrent blockchain network scenarios. Its innovative responsibility evaluation system and grouping hierarchical network model provide strong technical support for the further development of blockchain technology.

4. Conclusion

Through in-depth discussion and comparison of distributed consensus algorithms based on blockchain, this study puts forward a series of innovative performance optimization methods, especially for the performance bottlenecks faced by PoW and PoS. These optimization methods include improved DPoS algorithm based on node responsibility monitoring, hybrid distributed consensus and P2P network optimization, PB-RAFT algorithm based on parallel batch processing and ER-PBFT algorithm based on regional representative participation consensus. The experimental results show that Tower BFT-DPoSR algorithm performs well in key performance indexes such as throughput, confirmation time, energy consumption, decentralization degree, security and fault tolerance, and is significantly superior to traditional DPoS and other optimization algorithms. In addition, by comprehensively analyzing the advantages and disadvantages of existing consensus algorithms and combining with the latest research results, the targeted optimization strategy proposed in this paper not only improves the transaction processing capacity of blockchain system and reduces energy consumption, but also further enhances the decentralization and security of blockchain, laying a solid foundation for the wide application of blockchain technology. This study not only provides scientific basis and practical guidance for improving the performance of blockchain technology, but also lays a solid foundation for building a more efficient, safe and extensible blockchain ecosystem.

Acknowledgements

In 2022, the Education Department of Fujian Province, Research on the Application Technology of Distributed Database Based on Blockchain, (JAT220833)

References

[1] Wang, W. , & Sun, J. (2024). Distributed new energy system access based on blockchain consensus algorithm. International Journal of Emerging Electric Power Systems, 25(4), 533-540.

[2] Li, S. , Zhang, H. , Chen, Z. , Wang, J. , & Song, B. (2024). Enterprise composite blockchain double layer consensus algorithm based on improved dpos and bft. Peer-to-Peer Networking and Applications, 17(3), 1682-1701.

[3] Shen, T. , Li, T. , & Zhang, B. C. (2023). Gt-nrsm: efficient and scalable sharding consensus mechanism for consortium blockchain. Journal of supercomputing, 79(17), 20041-20075.

[4] Bansal, V. , Baliyan, N. , & Ghosh, M. (2024). Mlchain: a privacy-preserving model learning framework using blockchain. International Journal of Information Security, 23(1), 649-677.

[5] Ge, Y. , Zhang, W. , Li, H. , & Xie, Z. (2024). Traceability analysis of distributed new energy system access to green power based on blockchain consensus algorithm. International Journal of Emerging Electric Power Systems, 25(4), 523-532.

[6] Suo, Y. , Wang, Y. , & Luo, Q. Z. J. (2022). Sv-pbft: an efficient and stable blockchain pbft improved consensus algorithm for vehicle-to-vehicle energy transactions. Journal of Internet Technology, 23(6), 1191-1201.

[7] Ayenew, M. , Lei, H. , Li, X. , Weizhong, Q. , Abeje, E. , & Xiang, W. , et al. (2022). Enhancing the performance of permissionless blockchain networks through randomized message-based consensus algorithm. Peer-to-Peer Networking and Applications, 16(2), 499-519.

[8] Sun, Y. , Yan, B. , Yao, Y. , & Yu, J. (2021). Dt-dpos: a delegated proof of stake consensus algorithm with dynamic trust. Procedia Computer Science, 187(9), 371-376.

[9] Zheng, X. , Feng, W. , Huang, M. , & Feng, S. (2021). Optimization of pbft algorithm based on improved c4.5. Mathematical Problems in Engineering, 2021(2), 1-7.