


Hybrid Consensus Model for Blockchain Networks: Integrating Raft and PBFT for Enhanced Scalability and Performance

Zeqi Wang ^a

Faculty of Information Technology, Monash University, Clayton, Australia

Keywords: Hybrid Consensus Model; Raft Algorithm; PBFT; Blockchain Networks.


Abstract: This research investigates the integration of Reliable, Replicated, Redundant, And Fault-Tolerant (Raft) algorithm and Practical Byzantine Fault Tolerance (PBFT) consensus mechanisms to address scalability and performance limitations in blockchain networks, with a focus on financial applications. The objective is to develop a hybrid consensus model that combines Raft's efficient and rapid consensus process with PBFT's robust fault tolerance. The proposed model leverages Raft's decentralized voting procedure to improve system responsiveness while utilizing PBFT to ensure secure and accurate data consensus in environments prone to Byzantine faults. Extensive simulations were conducted to evaluate the hybrid model's performance. The results demonstrate that integrating Raft and PBFT not only preserves high throughput and reliability but also significantly enhances scalability, making the model particularly suitable for complex and security-sensitive applications, such as payment systems and digital currencies. This research highlights the practical benefits of hybrid consensus models in overcoming the inherent challenges of deploying blockchain technology in critical financial services. It suggests future research directions for broader applications across various sectors that require robust, scalable, and secure blockchain solutions.

1 INTRODUCTION

Blockchain technology's most well-known application in the financial sector is Bitcoin, first introduced by Satoshi Nakamoto in 2008 (Nakamoto, 2008). As this technology continues to evolve, it has spurred numerous innovations that are bringing profound changes to key financial areas such as payment systems and securities trading (Javaid et.al, 2022). While Bitcoin and Ethereum pioneered decentralized digital currencies, later technologies like Ripple and Stellar were specifically designed to address cross-border payments. As Pahlajani et al. suggest, these newer platforms adopt different consensus algorithms to enhance transaction efficiency and security, marking a significant advancement in blockchain's application to global finance (Pahlajani et.al, 2019). This evolution demonstrates how blockchain technology is being tailored to meet specific financial sector needs beyond its original cryptocurrency use case. Blockchain platforms such as Ripple and CoinExpress illustrate the potential to streamline

financial transactions by reducing intermediaries, lowering costs, and enhancing security through decentralized ledgers and efficient payment routing mechanisms. These improvements address the limitations of traditional systems like Society for Worldwide Interbank Financial Telecommunications (SWIFT), which, while highly secure and standardized, face challenges in terms of transaction speed, transparency, and costs due to their reliance on multiple intermediaries (Pahlajani et.al, 2019; Qiu et.al, 2019; Yu et.al, 2018). The contrast between blockchain-based solutions and traditional financial systems highlights the transformative potential of this technology in reshaping global financial infrastructure.

Despite advancements in blockchain technology that ensure transaction integrity and non-repudiation through decentralized architecture and digital signatures, its broader application in payment systems is hindered by challenges related to efficiency, security, scalability, and limited transaction speed. These issues are especially pronounced in high-throughput environments, where processing large

^a <https://orcid.org/0009-0007-7989-5642>

volumes of real-time transactions requires efficient consensus mechanisms that are difficult to implement without compromising decentralization, as noted by Kim and Kim (Kim et.al, 2020). However, consensus algorithms like Reliable, Replicated, Redundant, And Fault-Tolerant (Raft) and Practical Byzantine Fault Tolerance (PBFT) offer specific strengths that can help address these scalability and performance challenges (Yang et.al, 2022).

The Raft algorithm is characterized by its simplicity, efficiency, and low latency, making it commonly used in real-time transaction processing within private blockchains. As for PBFT, Yang et al. argue that its robust fault tolerance ensures data consistency even in the presence of malicious nodes, a feature that is crucial for maintaining the security and reliability of consortium blockchains (Yang et.al, 2022). Despite their individual merits, both Raft and PBFT face inherent limitations. Raft's simplicity may lead to insufficient fault tolerance, while PBFT, due to its high communication overhead and scalability issues, may perform less efficiently in larger networks.

This study proposes a hybrid consensus model that combines the advantages of both the Raft algorithm and PBFT to address the limitations of existing consensus mechanisms. Wang et al. demonstrated the feasibility of integrating multiple algorithms for robust and scalable digital payment solutions, this research takes a step further (Wang et.al, 2023). The proposed hybrid model leverages the efficiency of Raft and the fault tolerance of PBFT to enhance the performance, scalability, and security of blockchain-based payment systems.

As a new consensus mechanism, the integration of Raft and PBFT not only accelerates transaction processing and reduces latency but also ensures secure financial transactions. By addressing the limitations of current blockchain applications in the financial sector, this research contributes to the development of more efficient, secure, and scalable blockchain technologies. The resulting model is expected to significantly improve the practical implementation of blockchain systems in real-world financial scenarios.

2 METHODOLOGIES

This study focuses on developing a resilient system for high-volume payment processing by integrating the Raft and PBFT algorithms into a hybrid consensus model. Figure 1 illustrates a structured diagram of the hybrid model, showcasing the integration of Raft and

PBFT for blockchain applications. The model combines Raft's efficiency and simplicity in leader election and log replication with PBFT's robustness in ensuring data consistency and fault tolerance under malicious conditions. This hybrid approach seeks to address the limitations and strengths of each algorithm—specifically, Raft's lack of BFT and PBFT's challenges with scalability and communication overhead. By merging these characteristics, the model aims to achieve a balanced solution that enhances both performance and security. The ultimate goal is to implement this hybrid consensus model in high-volume, security-critical payment systems to ensure optimal performance and robust security.

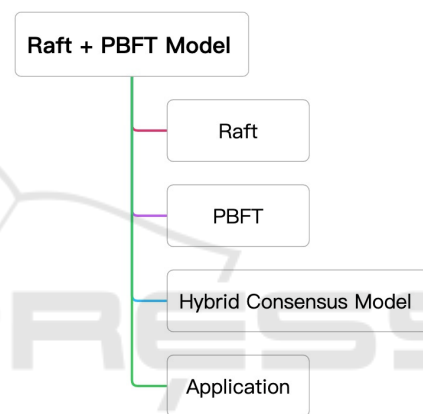


Figure 1: The structure of this model (Picture credit: Original).

2.1 Raft

The Raft consensus algorithm is recognized for its simplicity, high throughput, and low latency, making it particularly suitable for private blockchains. According to Huang et al., Raft's leader-based approach ensures efficient log replication, reliable leader election, and robust safety features, contributing to its reliable consensus and optimal resource utilization. Similarly, Macpherson and Goodell highlight Raft's effectiveness in blockchain redesigns, using it to enhance efficiency and focus functionality based on its proven performance (Macpherson et.al, 2024). However, Raft is not designed to handle BFT scenarios, as it assumes that failures are non-malicious (i.e., crash failures), meaning nodes may stop but will not behave maliciously. This limitation affects Raft's applicability in environments where nodes might act

arbitrarily or maliciously, such as those prone to Byzantine faults (Ongaro and Ousterhout, 2014).

2.2 PBFT

PBFT is a consensus algorithm widely used in blockchain alliance chains, introduced by Castroin 1999 as an improvement over the original BFT algorithm (Castro and Liskov, 1999). Yang et al. consider PBFT to be the most prevalent consensus algorithm for blockchain alliance chains but highlight significant limitations in terms of scalability, communication complexity, and fault tolerance (Yang et.al, 2022). These issues, they argue, confine PBFT's effectiveness to smaller networks, making it less suitable for larger and more demanding applications, such as financial services. Similarly, Zhang and Li recognize that PBFT's three-phase commit protocol leads to substantial communication overhead, especially in large-scale systems with numerous nodes, which ultimately limits its overall efficiency (Zhang and Li, 2018).

2.3 Hybrid Consensus Model

Before delving into the hybrid consensus model integrating Raft and PBFT, it is essential to explore other notable hybrid models that have been implemented in blockchain technology. These models demonstrate how different consensus algorithms can be combined to enhance performance, scalability, and security. Kwon outlines a hybrid model that integrates Tendermint's BFT consensus with Proof of Stake (PoS) to eliminate the need for energy-intensive mining, as seen in Proof of Work (PoW) systems like Bitcoin (Kwon, 2014). This model leverages BFT for fast and secure consensus finality, while PoS ensures that validators with a stake in the network maintain its security and stability by locking up their coins, aligning their interests with the network's well-being. Zhang et al. propose a hybrid model for Central Bank Digital Currency (CBDC) that integrates Delegated Proof of Stake (DPOS) and PBFT to enhance transaction throughput and scalability (Zhang et.al, 2021). The model combines an account-based system for handling frequent, small transactions with an unspent transaction output (UTXO) model for managing larger, less liquid assets, while employing a modular architecture that optimizes node functionality.

Following the exploration of these hybrid models, this research focuses on a new hybrid consensus model that integrates Raft and PBFT to address the efficiency and scalability challenges common in

payment systems. By combining Raft's low-latency consensus mechanism with PBFT's ability to BFT, the model ensures both performance and security in high-throughput environments.

3 RESULT AND DISCUSSION

The discussion section will evaluate the advantages and drawbacks of both the Raft and PBFT models, while also exploring future research directions. Focusing initially on Raft, its unique qualities such as simplicity, high throughput, and low latency make it particularly well-suited for private blockchain networks like those developed by Macpherson and Goodell (Macpherson et.al, 2024). They have utilized Raft to redesign an innovative digital payment infrastructure that manages retail CBDCs, which enhances user privacy and enables direct asset custody. This system processes transactions in real-time without sacrificing reliability and data integrity, even under conditions where up to half of the network nodes fail. This resilience, praised by Huang et al. (Huang et.al, 2020), confirms Raft's suitability for environments requiring predictable and robust operations, particularly where nodes are non-malicious and extensive transaction verification is unnecessary.

Transitioning to PBFT, this algorithm ensures accurate data consensus within a distributed network, even amidst Byzantine nodes engaging in malicious activities, making it one of the most widely adopted consensus mechanisms. Building on PBFT's foundation, Yang et al. have developed Nested Byzantine Fault Tolerance (NBFT), which integrates a consistent hashing algorithm to improve node selection and grouping, thereby enhancing fault tolerance and scalability (Yang et.al, 2022). Similarly, Zhang and Li have proposed the Group-Hierarchy (GH) model based on PBFT, employing a layered approach to achieve both local and global consensus across divided groups within a system (Zhang and Li, 2018). This architecture streamlines the consensus process and exemplifies PBFT's flexibility and effectiveness when integrated with other models. Such adaptability is crucial for enhancing the overall effectiveness of consensus mechanisms in distributed systems, including potential synergies between Raft and PBFT.

Zhang et al. proposed a hybrid model known as Proof of Authority-Practical Byzantine Fault Tolerance (POA-PBFT), which is a fusion of Proof of Authority and PBFT (Zhang et.al, 2021). This model enhances the traditional DPOS-BFT by specifically

tailoring the block production sequence and consensus mechanisms for CBDCs. This design significantly bolsters the security and efficiency of the blockchain network. Unlike Raft's decentralized voting process where nodes democratically elect a leader, POA-PBFT uses a central authority to appoint bookkeeping nodes, simplifying the election process and ensuring stable node operations. This centralized appointment mechanism is particularly suited to the unique requirements of CBDCs, ensuring controlled and stable operations within the blockchain environment tailored for digital currencies managed by central banks. The Raft-PBFT hybrid model presents a more suitable option for blockchain applications by combining Raft's decentralized voting process with PBFT's stringent control mechanisms. This synergy allows the model to benefit from Raft's streamlined leader election process, enhancing system responsiveness and robustness, while also incorporating PBFT's capacity to ensure accurate data consensus in the presence of Byzantine faults. Consequently, this hybrid model capitalizes on the strengths of both consensus mechanisms, enhancing the overall reliability and efficiency of the system. This makes it a particularly effective solution for complex blockchain environments, especially within payment system.

4 CONCLUSIONS

This study investigated the integration of Raft and PBFT consensus algorithms to address scalability and performance issues in blockchain networks, particularly within the financial sector. The proposed hybrid consensus model combines Raft's efficiency with PBFT's robust fault tolerance, aiming to optimize blockchain-based payment systems. By thoroughly analyzing the advantages and limitations of each algorithm, the research introduces a synergistic solution that overcomes existing limitations and enhances transaction processing speed, system reliability, and scalability.

Future research will focus on designing and implementing this hybrid consensus model to validate its applicability in real-world payment systems. This will include conducting detailed simulations and experimental tests to assess the model's performance in managing the complexities of actual financial transactions. Additionally, subsequent studies will address potential challenges during the implementation and operational phases, such as integrating the distinct consensus mechanisms of Raft

and PBFT and ensuring their cohesive operation within a unified system.

REFERENCES

- Castro, M., Liskov, B., 1999. Practical byzantine fault tolerance. *OsDI*. 99(1999), 173-186.
- Huang, D., Ma, X., Zhang, S., 2020. Performance analysis of the raft consensus algorithm for private blockchains. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 50(1), 172-181.
- Javaid, M., Haleem, A., Singh, R.P., et al. 2022. A review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, 2(3), 100073.
- Kim, S.I., Kim, S.H., 2020. E-commerce payment model using blockchain. *Journal of Ambient Intelligence and Humanized Computing*, 13(3), 1673-1685.
- Kwon, J., 2014. Tendermint: Consensus without mining. *Draft v. 0.6, fall*, 1(11), 1-11.
- Macpherson, W., Goodell, G., 2024. Benchmarking the performance of a self-custody, non-ledger-based, obliviously managed digital payment system. *arXiv preprint: 2404.12821*.
- Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. Satoshi Nakamoto.
- Ongaro, D., Ousterhout, J., 2014. In search of an understandable consensus algorithm. *USENIX annual technical conference*, 305-319.
- Pahlajani, S., Kshirsagar, A., Pachghare, V., 2019. Survey on private blockchain consensus algorithms. *International Conference on Innovations in Information and Communication Technology*, 1-6.
- Qiu, T., Zhang, R., Gao, Y., 2019. Ripple vs. SWIFT: Transforming cross border remittance using blockchain technology. *Procedia computer science*, 147, 428-434.
- Wang, Z.F., Liu, S.Q., Wang, P., et al. 2023. BW-PBFT: Practical byzantine fault tolerance consensus algorithm based on credit bidirectionally waning. *Peer-to-Peer Networking and Applications*, 16(6), 2915-2928.
- Yang, J., Jia, Z., Su, R., et al. 2022. Improved fault-tolerant consensus based on the PBFT algorithm. *Ieee Access*, 10, 30274-30283.
- Yu, R., Xue, G., Kilari, V.T., et al. 2018. CoinExpress: A fast payment routing mechanism in blockchain-based payment channel networks. *International conference on computer communication and networks*, 1-9.
- Zhang, J., Tian, R., Cao, Y., et al. 2021. A hybrid model for central bank digital currency based on blockchain. *IEEE Access*, 9, 53589-53601.
- Zhang, L., Li, Q., 2018. Research on consensus efficiency based on practical byzantine fault tolerance. *International conference on modelling, identification and control*, 1-6.