Integrated Science

Journal of Integrated
SCIENCE & TECHNOLOGY

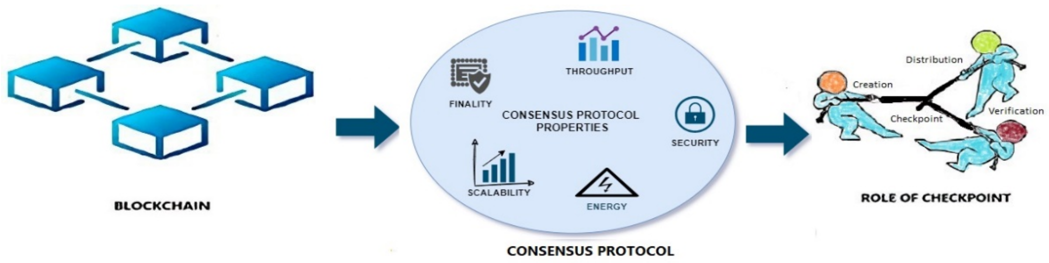
Enhancing efficiency and scalability in Blockchain Consensus algorithms: The role of Checkpoint approach

Priyanka Chorey,* Neeraj Sahu

Computer Science and Engineering, G. H. Raisoni University, Amravati, India.

Received on: 23-May-2023, Accepted and Published on: 11-Aug-2023

ABSTRACT



Blockchain technology has gained significant attention due to its potential to revolutionize various industries by providing decentralized, transparent, and secure systems. However, the scalability and efficiency challenges faced by traditional blockchain consensus algorithms have hindered widespread adoption. Consensus algorithms play a crucial role in achieving agreement among network participants regarding the validity and ordering of transactions. Traditional consensus algorithms like Proof of Work (PoW) and Proof of Stake (PoS) have shown limitations in terms of their resource-intensive nature, slow transaction processing, and limited scalability. This paper presents efficiency and scalability is critical considerations in blockchain consensus algorithms. The utilization of checkpoint mechanisms offers promising avenues for enhancing the performance of consensus protocols. The role and purpose of checkpoint approach, areas of improvement, research direction in the field of blockchain technology.

Keywords: Blockchain Consensus Algorithms, Checkpoint Approach, Security, Checkpoint Mechanism.

INTRODUCTION

Blockchain technology has emerged as a transformative innovation with the potential to revolutionize various industries, including finance, supply chain, healthcare, and more.[1,9] At its core, blockchain is a decentralized and distributed ledger that maintains a record of transactions across multiple network participants.[14,20] The integrity and security of the blockchain rely on achieving consensus among these participants.[3] Consensus algorithms are fundamental to blockchain systems as they enable network participants to agree on the validity of transactions and maintain a consistent view of the distributed ledger.[14] However, achieving efficient and scalable consensus algorithms in blockchain poses significant challenges.[13,22]

Background

Efficiency refers to the ability to process a large number of transactions quickly and with minimal computational overhead. Scalability, on the other hand, pertains to the ability of a blockchain system to handle an increasing number of participants and transactions without compromising performance or resource requirements.[1,6] The decentralized nature of blockchain, where every participant maintains a copy of the ledger and participates in the consensus process, creates inherent difficulties in achieving efficiency and scalability.[14] Traditional consensus algorithms, such as proof-of-work (PoW) and proof-of-stake (PoS), have been widely used but are associated with limitations in terms of computational costs, energy consumption, and transaction throughput.[32] As blockchain technology continues to evolve and gain adoption, it becomes crucial to develop innovative approaches

*Corresponding to: Priyanka Chorey
Email: priyankachorey07@gmail.com

Cite as: *J. Integr. Sci. Technol., 2024, 12(1), 706.*
URN:NBN:sciencein.jist.2024.v12.706

ISSN: 2321-4635
http://pubs.thesciencein.org/jist

that can enhance the efficiency and scalability of consensus algorithms.[6,19] A key aspect of addressing these challenges is the exploration of checkpoint mechanisms.[25] Checkpoint mechanisms in blockchain systems involve periodic snapshots of the blockchain state.[8] These snapshots act as reference points that allow participants to skip unnecessary computations and validate transactions efficiently. By reducing the computational overhead required to verify the entire transaction history, checkpoint approaches have the potential to significantly improve the efficiency and scalability of consensus algorithms.[3,6] The significance of enhancing efficiency and scalability in blockchain consensus algorithms is twofold.[14] First, it enables blockchain systems to handle a larger number of transactions, accommodating growing user demands and supporting real-world applications at scale.[28,33] This is especially crucial in industries with high transaction volumes, such as finance and supply chain, where the ability to process a large number of transactions quickly is essential. Second, improving efficiency and scalability can lead to reduced costs, both in terms of computational resources and energy consumption. This can make blockchain systems more sustainable and economically viable, fostering wider adoption across industries.[1] By exploring the role of checkpoint approaches in enhancing efficiency and scalability in blockchain consensus algorithms, researchers and practitioners can contribute to the development of more robust and scalable blockchain solutions.[3,13] Such advancements can unlock the full potential of blockchain technology and drive its widespread adoption in diverse sectors, ultimately transforming how business processes and transactions are conducted globally.[9,31]

Blockchain Technology and Its potential Impact

Blockchain technology is a decentralized and distributed ledger that records transactions across multiple computers, creating an immutable and transparent record of data.[20] It gained prominence with the introduction of Bitcoin, the first decentralized cryptocurrency, by the pseudonymous creator Satoshi Nakamoto in 2008. However, the scope and potential applications of blockchain extend far beyond cryptocurrencies.[9] At its core, a blockchain consists of a chain of blocks, where each block contains a set of transactions. These transactions are verified and added to the blockchain through a consensus mechanism, ensuring the integrity and security of the data.[8] The decentralized nature of blockchain, with no central authority or intermediary, makes it resistant to tampering and censorship. As blockchain technology continues to evolve, further advancements such as scalability solutions, interoperability, and privacy-enhancing techniques are being developed to address its limitations.[9,26] With ongoing research and innovation, blockchain holds the promise of transforming industries and creating new opportunities for businesses and individuals worldwide.[6,37]

Consensus Algorithms in Blockchain Systems

The importance of efficient and scalable consensus algorithms in blockchain systems cannot be overstated.[13,54] Consensus algorithms play a critical role in ensuring the integrity, security, and reliability of blockchain networks. They enable network participants to agree on the validity and order of transactions, maintain a consistent and tamper-resistant distributed ledger, and prevent malicious attacks and double-spending.[10] Efficient and scalable consensus algorithms are crucial for the successful implementation and widespread adoption of blockchain systems.[13] They enable high transaction throughput, fast and responsive network operation, resource efficiency, network scalability, enhanced security, and a positive user experience.[6] Continued research and innovation in consensus algorithms are vital to address the challenges and limitations of existing approaches, paving the way for the broader utilization of blockchain technology in diverse sectors.[9,42]

Challenges in Blockchain Consensus Algorithms

Blockchain consensus algorithms face several challenges that need to be addressed to ensure the efficiency, security, and scalability of blockchain networks shown in figure 1.[30] These challenges include:

- Scalability in blockchain consensus algorithms as participant and transaction numbers increase, necessitating efficient handling of the growing workload through solutions like sharding and off-chain transactions.[6]
- Consensus algorithms achieve high-performance and throughput by efficiently processing and validating a large number of transactions within a reasonable time frame, while mitigating latency and delays that can impact network performance.[12,16]

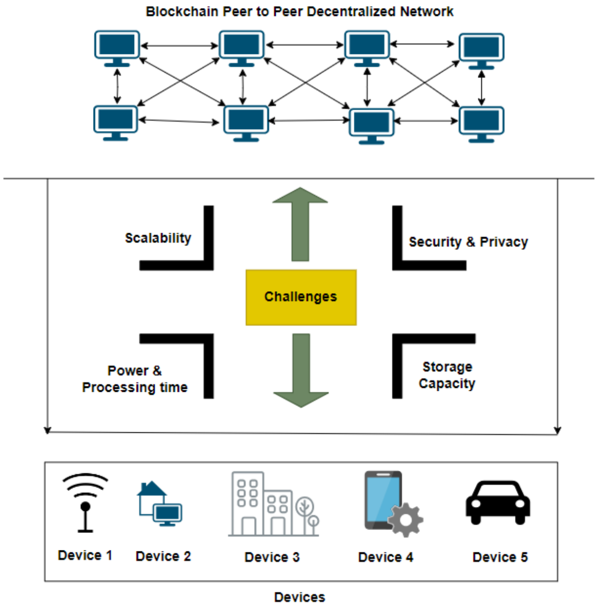


Figure 1 Challenges in Blockchain Consensus Algorithms

- Energy efficiency in consensus algorithms as traditional approaches like PoW consume high amounts of energy, necessitating the development of energy-efficient alternatives like PoS or PoA to promote sustainability in blockchain systems.[18]
- Ensuring security and resistance to attacks in consensus algorithms as they need to protect the blockchain network from

double-spending, Sybil attacks, and 51% attacks while maintaining decentralization and preventing the concentration of power for trust and security.[10]

- Decentralized governance in consensus algorithms poses challenges in achieving fair participation, consensus on protocol changes, and aligning incentives, which are addressed through governance models like on-chain voting and delegated consensus.[5]
- Privacy and confidentiality pose a challenge in consensus algorithms as they aim to maintain transparency and immutability while protecting sensitive data, with ongoing development of privacy-preserving techniques like zero-knowledge proofs and secure multi-party computation to address these concerns.[34,41,51,]
- Interoperability and cross-chain consensus pose when blockchain networks expands, requiring consensus algorithms to facilitate secure communication, data exchange, and interoperability among different chains while ensuring overall security and consensus.[21,48]

CHECKPOINT

The checkpoint approach is a technique used in blockchain consensus algorithms to enhance efficiency and scalability.[6]

It involves periodically creating checkpoints that summarize the state of the blockchain at a certain block height. These checkpoints serve as reference points, allowing nodes to verify the blockchain's integrity without having to validate the entire transaction history. By using checkpoints, consensus algorithms can reduce the computational and storage requirements for nodes to join the network or synchronize with it. Instead of starting from the genesis block and validating every transaction, new nodes can simply verify the checkpoints and continue from there. This approach significantly reduces the time and resources required to bootstrap a new node or recover from a network interruption.

In addition, checkpoints enable faster block propagation and validation. Instead of broadcasting each block individually, nodes can transmit a batch of blocks between checkpoints, reducing network overhead and improving throughput. Additionally, the verification process can be streamlined by validating transactions only within the range of the last checkpoint to the current block, further enhancing efficiency.[27] While the checkpoint approach offers benefits in terms of efficiency and scalability, it also introduces certain trade-offs.[6] The use of checkpoints centralizes trust to some extent, as nodes need to trust the authority responsible for generating and distributing checkpoints. Additionally, checkpoints require careful management to prevent manipulation or tampering that could compromise the blockchain's integrity.

Concept of Checkpoints in A Blockchain

The blockchain consists of a sequence of blocks, each containing multiple transactions (T_1, T_2, T_3, etc.). Block (1) and Block (2) represent individual blocks in the blockchain. A checkpoint is a specific block that is designated as a reference point for the blockchain's state. The checkpoint stores the hash of the block and is typically set periodically or based on predefined criteria.[24] Transactions are stored within the blocks, and the entire blockchain is linked together using cryptographic hashes.[23,46] In figure 2, the checkpoint serves as a verified and trusted reference point. By validating the blocks before the checkpoint, nodes in the blockchain network can more efficiently synchronize and validate the blockchain's integrity without having to go through the entire chain from the genesis block.[36]

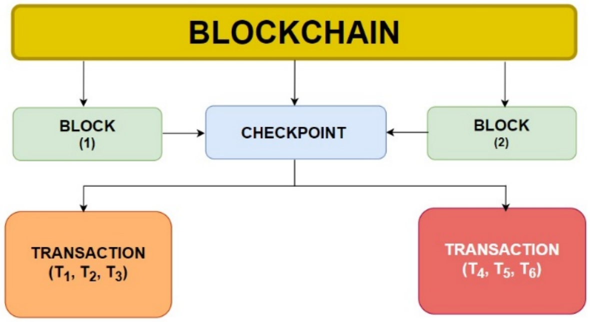

BLOCKCHAIN
BLOCK (1)
CHECKPOINT
BLOCK (2)
TRANSACTION (T_1, T_2, T_3)
TRANSACTION (T_4, T_5, T_6)

Figure 2 Simplified Representation of Checkpoint in Blockchain

Overview of Checkpoint Mechanism

The checkpoint mechanism is a technique used in blockchain systems to enhance efficiency, security, and scalability.[6] It involves periodically creating checkpoints that serve as reference points to verify the integrity of the blockchain without the need to validate the entire transaction history. The checkpoint mechanism as shown in figure 3 works as follows:

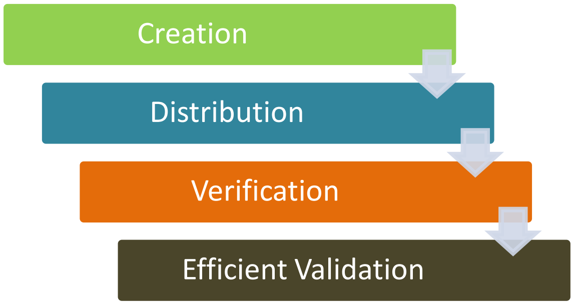


Figure 3 Checkpoint Mechanism

Checkpoint Creation: At specific intervals or block heights, checkpoints are generated by a trusted authority or a group of selected validators. These checkpoints summarize the state of the blockchain, including the hash of the block and other relevant information.

Checkpoint Distribution: The checkpoints are then distributed to the network participants, who can use them as a starting point for their validation process instead of starting from the genesis block. The distribution can be done through various methods, such as broadcasting the checkpoints through a peer-to-peer network or relying on a centralized authority.

Checkpoint Verification: Upon receiving the checkpoints, network participants verify their validity and integrity. This typically involves checking the cryptographic signatures of the checkpoints and ensuring they match the expected state of the blockchain.[2]

Efficient Validation: With the verified checkpoints, nodes can streamline the validation process. Instead of validating each transaction from the beginning, nodes can start their validation from the last checkpoint and validate only the transactions that occurred since then. This significantly reduces the computational and storage requirements for joining or synchronizing with the blockchain network.

Advantages:

- Improve efficiency by allowing new nodes to skip the validation of the entire transaction history, reducing the time and resources required for node bootstrapping and network recovery, resulting in faster node synchronization.
- Enhance scalability by reducing computational and storage requirements, enabling blockchain networks to handle a larger volume of transactions and participants more efficiently.[6]
- Enhance security by serving as trusted reference points for verifying the integrity of the blockchain. Participants can rely on verified checkpoints to ensure the authenticity and validity of transactions, maintaining the overall security of the blockchain network.
- It enables faster validation, reduces resource requirements, and enables blockchain networks to accommodate growing transaction volumes and participant numbers.

Role and Purpose

- Checkpoints serve as trusted reference points that include block hashes and relevant information to verify the integrity and immutability of the blockchain, ensuring it remains unaltered and secure.
- Checkpoints streamline bootstrapping and synchronization by enabling new nodes to validate from the last checkpoint, reducing computational and storage requirements by skipping full transaction history validation.
- Checkpoints expedite node synchronization by allowing new nodes to join the network at the latest verified checkpoint, accelerating the process by bypassing the validation of the entire transaction history and saving time and resources.
- Checkpoints boost scalability in consensus algorithms and blockchain networks by reducing validation workload, facilitating handling of increased transaction volumes and participant numbers with network growth.[6]
- Checkpoints provide a level of trust and security to the consensus algorithm. Participants can rely on the verified checkpoints as a reference point to ensure the authenticity and validity of the blockchain. By trusting the checkpoints, participants can have confidence that the transactions since the last checkpoint are valid and the network's integrity is maintained.[54]
- Checkpoints play a critical role in consensus algorithms by providing reference points for integrity verification, improving efficiency, enhancing synchronization, boosting scalability, and ensuring security.[6] They are valuable tools that contribute to the overall performance and reliability of the blockchain network.[12,35]

Checkpoint Based Approaches

By utilizing checkpoints, these approaches reduce the validation workload by allowing nodes to skip the validation of the entire transaction history. Instead, nodes can start validation from the last verified checkpoint, significantly improving the efficiency of synchronization and bootstrapping processes. This reduction in computational and storage requirements enables the network to handle a larger number of transactions and participants, enhancing scalability.[12] By streamlining the validation process, checkpoint-based approaches contribute to the overall efficiency and scalability of blockchain consensus algorithms. Figure 4 illustrates checkpoint based approaches in blockchain discuss below briefly are as follows.

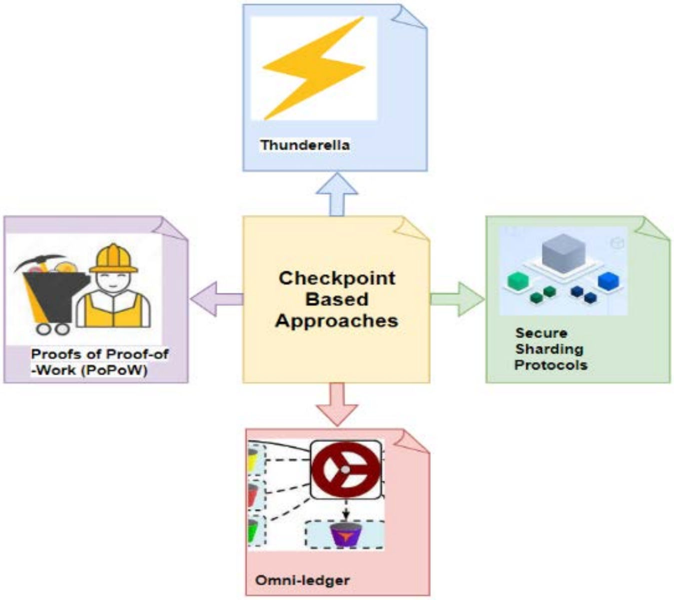

Thunderella
Proofs of Proof-of-Work (PoPoW)
Checkpoint Based Approaches
Secure Sharding Protocols
Omni-ledger

Figure 4 Blockchain Checkpoint Based Approaches

Thunderella

Thunderella is a consensus algorithm designed to improve the efficiency and scalability of blockchain systems.[7] It is a hybrid consensus protocol that combines elements of both proof-of-work (PoW) and proof-of-stake (PoS) mechanisms.[4,50] In Thunderella, the blockchain network is divided into multiple shards, with each shard containing a subset of nodes responsible for validating transactions within that shard. Thunderella utilizes a PoW-based mechanism to reach consensus within each shard, where a randomly selected leader node proposes a block and other nodes validate it through a lightweight PoW computation.[7] To achieve cross-shard consensus, Thunderella introduces a concept called "thunder" blocks.[7] Thunder blocks act as checkpoints that provide a summary of the state and transactions within each shard. The leader of each shard includes a hash of the shard's thunder block in the next shard's block, forming a chain of thunder blocks across shards. This enables the synchronization of states between shards and ensures the overall consistency of the blockchain. The Thunderella consensus algorithm addresses the scalability challenge by parallelizing transaction processing across multiple shards.[7] It reduces the validation workload within each shard and enhances the overall transaction throughput of the blockchain network.[6] Additionally, Thunderella provides a mechanism for efficient cross-shard communication and synchronization through the use of thunder blocks.[42] By combining the benefits of PoW and PoS, Thunderella aims to achieve a balance between security, decentralization, and scalability in blockchain consensus.[8] It offers a promising approach to address the scalability limitations of traditional blockchain systems while maintaining a high level of security and decentralization.[7]

Proofs of Proof-of-Work (PoPoW)

PoPoW is a cryptographic construction that enables the verification of a "proof-of-work" solution within another blockchain network. It allows for the transfer of the computational effort (proof-of-work) performed in one blockchain to another blockchain as evidence of a valid and costly computation. The concept of PoPoW originated from the desire to establish a connection between different blockchain networks and leverage the security of an established blockchain (often referred to as the "source chain") to enhance the security of a new or less secure blockchain (often referred to as the "target chain"). In PoPoW, a participant from the source chain creates a proof-of-work solution, typically a valid block, and then constructs a cryptographic proof that encapsulates the entire chain's history from the genesis block up to and including the desired block.[2] This proof is then submitted to the target chain as evidence of the computational effort expended on the source chain. Upon receiving the PoPoW proof, participants in the target chain can efficiently validate the proof by verifying the chain history, the proof-of-work solution, and the cryptographic integrity of the proof itself. If the validation is successful, the target chain can consider the proof as sufficient evidence of the computational work performed on the source chain, which enhances the security of the target chain. PoPoW provides a mechanism for cross-chain communication and allows a blockchain network to benefit from the accumulated computational power and security of another established network.[8,15] It enables interoperability between different blockchain systems and can be used to reinforce the security of less secure chains by leveraging the consensus strength of more established chains. Overall, PoPoW serves as a bridge between blockchain networks, enabling the transfer of computational effort and security between them through cryptographic proofs. It offers a solution to enhance the trust, security, and interoperability of blockchain systems.

Secure Sharding Protocols

In this approach, the blockchain network is divided into smaller subsets called shards, with each shard responsible for processing a subset of transactions.[47] To maintain consistency and integrity across shards, periodic checkpoints are established at specific intervals. Checkpoints serve as reference points that summarize the state of each shard at a particular block height. They include information such as the hash of the last validated block, shard state information, and other relevant data. Checkpoints provide a verifiable and tamper-proof reference to ensure the authenticity and validity of the blockchain.[41] The checkpoint-based approach allows new nodes or nodes resynchronizing with the network to start their validation process from the last verified checkpoint. By skipping the validation of the entire transaction history, the computational and storage requirements are significantly reduced, facilitating more efficient bootstrapping and synchronization of new nodes. The use of checkpoints also enables the network to handle a larger number of transactions and participants by reducing the validation workload within each shard. This enhances the scalability of the consensus algorithm and the overall blockchain network.[6] The checkpoint-based approach contributes to the security and attack resistance of the network. By trusting the verified checkpoints as reference points, participants can have confidence in the authenticity and integrity of the transactions since the last checkpoint. This helps prevent double-spending attacks, Sybil attacks, and other malicious activities.[10] It allows for parallel processing across shards, reduces validation workload, and provides trusted reference points for maintaining the integrity of the blockchain.[48]

Omni-ledger

Omni-ledger is a blockchain protocol that utilizes a checkpoint-based approach to enhance scalability, efficiency, and security in consensus algorithms.[5] The Omni-ledger checkpoint-based approach combines concepts such as sharding, periodic checkpoints, and cross-checkpoint consistency to achieve these goals. The blockchain network is partitioned into multiple shards, with each shard responsible for processing a subset of transactions. Periodic checkpoints are established at regular intervals across the shards.[11] Checkpoints in Omni-ledger include the aggregated state of the shard, such as the Merkle root of the shard's transaction history and other relevant information. The checkpoint-based approach in Omni-ledger serves several purposes.[45] Firstly, it allows for efficient synchronization of nodes joining or rejoining the network. New nodes can start their validation process from the most recent verified checkpoint, reducing the computational and storage requirements by skipping the validation of the entire transaction history. Secondly, checkpoints in Omni-ledger enable efficient cross-checkpoint consistency.[44] To maintain the integrity of the blockchain, checkpoints are periodically validated by other shards. This cross-checkpoint consistency ensures that all shards have an up-to-date and consistent view of the blockchain, preventing inconsistencies or forks. The checkpoint-based approach in Omni-ledger enhances the scalability of the consensus algorithm.[46] By dividing the network into shards and utilizing checkpoints, the validation workload is distributed across shards, allowing for parallel processing of transactions and increasing the transaction throughput of the network.[40,47] The checkpoint-based approach in Omni-ledger also contributes to security. Checkpoints serve as reference points for validating the integrity of the blockchain. By relying on verified checkpoints, participants can have confidence in the authenticity and validity of the transactions since the last checkpoint, reducing the risk of attacks such as double-spending.[10] It enables efficient node synchronization, maintains consistency across shards, enhances scalability, and provides a trusted reference point for transaction validation.[29]

DISCUSSION

The checkpoint approach plays a crucial role in enhancing the efficiency and scalability of blockchain consensus algorithms.[6] By introducing checkpoints at specific intervals, the validation workload can be significantly reduced, leading to improved efficiency in the blockchain network.[49] One of the primary challenges in blockchain consensus algorithms is scalability.[6] As the number of participants and transactions increases, traditional consensus algorithms like proof-of-work (PoW) can become slower and resource-intensive. The checkpoint approach addresses this challenge by allowing nodes to skip the validation of the entire transaction history and start validation from the last verified checkpoint.[52] This reduces the computational and storage requirements, enabling more efficient bootstrapping and synchronization of new nodes.The checkpoints contribute to the scalability of the consensus algorithm by distributing the validation workload across checkpoints.[6] Instead of each node validating every transaction, nodes can focus on validating transactions since the last checkpoint, allowing for parallel processing and increasing the transaction throughput of the network. In addition to efficiency and scalability, the checkpoint approach also enhances the security and integrity of the blockchain network.[43] By including the hash of the block and relevant information, checkpoints serve as trusted reference points for validating the authenticity and validity of the blockchain. Participants can rely on these checkpoints to ensure that the blockchain has not been modified or tampered with, enhancing trust and security in the network.[53]

Moreover, the checkpoint approach enables efficient cross-checkpoint consistency. Periodic validation of checkpoints by other shards or nodes helps maintain the integrity of the blockchain and prevents inconsistencies or forks. This ensures that all shards have an up-to-date and consistent view of the blockchain, contributing to the overall reliability of the network.

However, it is important to note that the checkpoint approach is not without its challenges. Determining the appropriate frequency and size of checkpoints requires careful consideration to strike a balance between efficiency and security. In addition, the design and implementation of checkpoint mechanisms should be robust to withstand attacks and ensure the immutability of the checkpoints themselves.[4]

Areas for Improvement

- Developing algorithms or models that dynamically adjust checkpoint intervals based on network conditions, transaction volume, or other relevant factors, optimizing the efficiency and scalability.
- Explore new techniques or protocols to improve the scalability of cross checkpoint consistency, enabling blockchain networks to handle larger transaction volumes and participant numbers while maintaining the integrity of the blockchain.[5]
- Developing advanced cryptographic techniques, such as zero-knowledge proofs or multi-party computation, and exploring new approaches for verifying checkpoint integrity, including decentralized or distributed validation mechanisms, to enhance the security.[4]
- Explore the integration of the checkpoint approach with other scalability solutions, such as sharding or off-chain transactions, to leverage their strengths and synergies, achieving greater scalability and efficiency in blockchain consensus algorithms.[11]
- Developing efficient algorithms, data structures, and protocols to minimize computational and storage overhead, and exploring practical deployment models that consider real-world constraints to improve the practicality and effectiveness.[5]

The role of checkpoint approach highlight the challenges, solutions, and considerations involved in selecting the most appropriate consensus algorithm for specific blockchain applications. The article's insights encourage a more informed and systematic approach to algorithm selection, ultimately contributing to the optimization of blockchain networks in terms of efficiency and scalability. Notably, the consensus algorithms that are the subject of the study share a common objective: achieving consensus within the network efficiently. This common goal is paramount for the seamless functioning of any blockchain system. The most of the researchers delve into the workings of Proof of Work (PoW) algorithms, which demand significant computational effort from participating nodes. However, the advent of specialized hardware has disrupted the level playing field in PoW-based networks, posing a challenge to the fairness of the system.[38]

To extends the realm of Proof of Stake (PoS) as a potential solution to the shortcomings of PoW. PoS is hailed as a more sustainable alternative due to its reduced energy consumption, yet it grapples with issues related to initial coin distribution and concerns regarding decentralization.[18] This work scrutinizes the feasibility of hybrid approaches that blend PoW and PoS, acknowledging their potential benefits while emphasizing the complexity they introduce to network architecture and protocol layers.[39]

The insights into the challenges, solutions, and ongoing developments in the field, ultimately pave the way for more informed decision-making processes in selection of consensus algorithms for diverse blockchain applications.

Future Scope

Research directions in enhancing efficiency and scalability in blockchain consensus algorithms through the checkpoint approach include:

- Optimizing checkpoint intervals.
- Improving cross-checkpoint consistency scalability.
- Enhancing security measures with advanced cryptographic techniques and decentralized validation mechanisms.[8]
- Integrating with other scalability solutions like sharding or off-chain transactions.[11]
- Addressing practical implementation considerations such as efficient algorithms, data structures, and deployment models.

CONCLUSION

The checkpoint approach plays a significant role in enhancing the efficiency and scalability of blockchain consensus algorithms. By providing trusted reference points, checkpoints streamline bootstrapping and synchronization, reducing computational and storage requirements. They contribute to the scalability of consensus algorithms by reducing the validation workload, enabling the network to handle increased transaction volumes and participant numbers. Additionally, checkpoints enhance the security and integrity of the blockchain by serving as anchor points for validation.

However, there are areas for improvement and innovation in this approach. Optimization of checkpoint intervals, scalability of cross-checkpoint consistency, enhanced security measures, integration with other scalability solutions, and practical implementation considerations are potential research directions that can further enhance the efficiency and scalability of the checkpoint-based approach. Overall, the checkpoint-based approach holds great promise in advancing the efficiency, scalability, and security of blockchain networks, paving the way for broader adoption and utilization in various industries.

Acknowledgments

The authors thank the editor and the reviewers for their valuable suggestions which helped in improving the paper's quality. We are thankful to Computer Science Engineering Department, G. H. Raisoni University, Amravati, Maharashtra, INDIA for providing all state-of-art facilities to carry out the research work in Research Laboratory.

Conflict of interest

Authors do not have any conflict of interest in publishing of this work. No Academic or financial interest to be declared for this work.

References and notes

1. U. Javaid, B. Sikdar. A Checkpoint Enabled Scalable Blockchain Architecture for Industrial Internet of Things. *IEEE Trans. Ind. Informatics* **2021**, 17 (11), 7679–7687.
2. S.S. Hazari, Q.H. Mahmoud. Improving transaction speed and scalability of blockchain systems via parallel proof of work. *Futur. Internet* **2020**, 12 (8), 125.
3. J. Nijsse, A. Litchfield. A taxonomy of blockchain consensus methods. *Cryptography* **2020**, 4 (4), 1–15.
4. B. Lashkari, P. Musilek. A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access.* 2021, pp 43620–43652.
5. L. Zhang, L. Hang, D. Kim. Enhanced Multiset Consensus Protocol Based on PBFT for Logistics Information Traceability. *Secur. Commun. Networks* **2023**, 2023.
6. K. Cong, Z. Ren, J. Pouwelse. A Blockchain Consensus Protocol with Horizontal Scalability. In *17th International IFIP TC6 Networking Conference, Networking 2018*; Zurich, Switzerland, **2018**; pp 424–432.
7. R. Pass, Shi. Elaine.Thunderella: Blockchains with Optimistic Instant Confirmation. In *In book: Advances in Cryptology – EUROCRYPT 2018*; pp 3–33.
8. D. Çulha. A Random and Scalable Blockchain Consensus Mechanism. *Asian J. Converg. Technol.* **2022**, 8 (1), 47.
9. A. Guru, B.K. Mohanta, H. Mohapatra, et al. A Survey on Consensus Protocols and Attacks on Blockchain Technology. *Appl. Sci.* **2023**, 13 (4), 2604.
10. S. Azouvi, G. Danezis, V. Nikolaenko. Winkle:Foiling Long-Range Attacks in Proof-of-Stake Systems. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies. Association for Computing Machinery*; New York, NY, USA; pp 189–201.
11. H. Luo. ULS-PBFT: An ultra-low storage overhead PBFT consensus for blockchain. *Blockchain Res. Appl.* **2023**, 100155.
12. H. Samy, A. Tammam, A. Fahmy, B. Hasan. Enhancing the performance of the blockchain consensus algorithm using multithreading technology. *Ain Shams Eng. J.* **2021**, 12 (3), 2709–2716.
13. T. Crain, C. Natoli, V. Gramoli. Red belly: A secure, fair and scalable open blockchain. *Proc. - IEEE Symp. Secur. Priv.* **2021**, 2021-May, 466–483.
14. A. Sarfaraz, R.K. Chakrabortty, D.L. Essam. The implications of blockchain-coordinated information sharing within a supply chain: A simulation study. *Blockchain Res. Appl.* **2023**, 4 (1), 100110.
15. G. Yu, B. Wu, X. Niu. Improved Blockchain Consensus Mechanism Based on PBFT Algorithm. In *Proceedings - 2020 2nd International Conference on Advances in Computer Technology, Information Science and Communications, CTISC 2020*; **2020**; pp 14–21.
16. P. Zhang, M. Zhou, Q. Zhao, A. Abusorrah, O.O. Bamasag. A Performance-Optimized Consensus Mechanism for Consortium Blockchains Consisting of Trust-Varying Nodes. *IEEE Trans. Netw. Sci. Eng.* **2021**, 8 (3), 2147–2159.
17. S. Chorey, N. Sahu. Failure recovery model in big data using the checkpoint approach. *J. Integr. Sci. Technol.* **2023**, 11 (4), 564.
18. M. Li, D. Hu, C. Lal, M. Conti, Z. Zhang. Blockchain-Enabled Secure Energy Trading with Verifiable Fairness in Industrial Internet of Things. *IEEE Trans. Ind. Informatics* **2020**, 16 (10), 6564–6574.
19. C. Qiu, F.R. Yu, H. Yao, et al. Blockchain-based software-defined industrial internet of things: A dueling deep q -learning approach. *IEEE Internet Things J.* **2019**, 6 (3), 4627–4639.
20. M. Ohara. A study on checkpointing for distributed applications using Blockchain-based data storage. In *Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing, PRDC*; IEEE, Kyoto, Japan, **2019**; Vol. 2019-December, pp 116–117.
21. K. Fan, H. Li, W. Jiang, C. Xiao, Y. Yang. Secure Authentication Protocol for Mobile Payment. *Tsinghua Sci. Technol.* **2018**, 23 (5), 610–620.
22. B.K. Zheng, L.H. Zhu, M. Shen, et al. Scalable and Privacy-Preserving Data Sharing Based on Blockchain. *J. Comput. Sci. Technol.* **2018**, 33 (3), 557–567.
23. Z. Qiao, Q. Yang, Y. Zhou, M. Zhang. Improved Secure Transaction Scheme with Certificateless Cryptographic Primitives for IoT-Based Mobile Payments. *IEEE Syst. J.* **2022**, 16 (2), 1842–1850.
24. P.J. Taylor, T. Dargahi, A. Dehghantanha, R.M. Parizi, K.K.R. Choo. A systematic literature review of blockchain cyber security. *Digit. Commun. Networks* **2020**, 6 (2), 147–156.
25. S. Zhou, K. Li, L. Xiao, et al. A Systematic Review of Consensus Mechanisms in Blockchain. *Mathematics* **2023**, 11 (10), 2248.
26. K.K.R. Choo, Z. Yan, W. Meng. Editorial: Blockchain in Industrial IoT Applications: Security and Privacy Advances, Challenges, and Opportunities. *IEEE Trans. Ind. Informatics* **2020**, 16 (6), 4119–4121.
27. I.T. Javed, F. Alharbi, T. Margaria, N. Crespi, K.N. Qureshi. PETchain: A Blockchain-Based Privacy Enhancing Technology. *IEEE Access* **2021**, 9, 41129–41143.
28. M. Shayan, C. Fung, C.J.M. Yoon, I. Beschastnikh. Biscotti: A Blockchain System for Private and Secure Federated Learning. *IEEE Trans. Parallel Distrib. Syst.* **2021**, 32 (7), 1513–1525.
29. E. Kokoris-Kogias, P. Jovanovic, L. Gasser, et al. OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding. In *Proceedings - IEEE Symposium on Security and Privacy*; San Francisco, CA, USA, **2018**; Vol. 2018-May, pp 583–598.
30. L. Cui, S. Yang, Z. Chen, et al. An Efficient and Compacted DAG-Based Blockchain Protocol for Industrial Internet of Things. *IEEE Trans. Ind. Informatics* **2020**, 16 (6), 4134–4145.
31. G. Guo, Y. Zhu, E. Chen, et al. Continuous improvement of script-driven verifiable random functions for reducing computing power in blockchain consensus protocols. *Peer-to-Peer Netw. Appl.* **2022**, 15 (1), 304–323.
32. A. Kaushik, A. Khatri. Systematic literature review on blockchain adoption in banking. *Pressacademia* **2021**, 8 (3), 126–146.
33. X. Su, Y. Liu, C. Choi. A Blockchain-Based P2P Transaction Method and Sensitive Data Encoding for E-Commerce Transactions. *IEEE Consum. Electron. Mag.* **2020**, 9 (4), 56–66.
34. J. Zhang, S. Zhong, T. Wang, H.C. Chao, J. Wang. Blockchain-based systems and applications: a survey. *J. Internet Technol.* **2020**, 21 (1), 1–14.

35. B.G. Pillai, J.A. Madhurya. A Decentralized Data Privacy for Mobile Payment using Blockchain Technology. *Int. J. Recent Technol. Eng.* **2020**, 8 (6), 5260–5264.
36. S.M.H. Bamakan, A. Motavali, A. Babaei Bondarti. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Syst. Appl.* **2020**, 154.
37. M. Andoni, V. Robu, D. Flynn, et al. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, 100, 143–174.
38. X. Meng, J. Xu, W. Liang, Z. Xu, K.C. Li. A lightweight anonymous cross-regional mutual authentication scheme using blockchain technology for internet of vehicles. *Comput. Electr. Eng.* **2021**, 95, 95,107431.
39. C. Allenbrand. Smart contract-enabled consortium blockchains for the control of supply chain information distortion. *Blockchain Res. Appl.* **2023**, 4 (3), 100134.
40. A.A. Abuhashim, C.C. Tan. Improving smart contract search by semantic and structural clustering for source codes. *Blockchain Res. Appl.* **2023**, 4 (2), 100117.
41. W. Liang, Y. Yang, C. Yang, et al. PDPChain: A Consortium Blockchain-Based Privacy Protection Scheme for Personal Data. *IEEE Trans. Reliab.* **2023**, 72 (2), 586–598.
42. S. Biswas, K. Sharif, F. Li, et al. PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain. *IEEE Internet Things J.* **2020**, 7 (3), 2343–2355.
43. Q. Xie, F. Dong, X. Feng. HLOChain: A Hierarchical Blockchain Framework with Lightweight Consensus and Optimized Storage for IoT. *Secur. Commun. Networks* **2023**, 2023, 3412200.
44. W. Zhou, H. Wang, G. Mohiuddin, D. Chen, Y. Ren. Consensus Mechanism of Blockchain Based on PoR with Data Deduplication. *Intelligent Automation and Soft Computing*. 2022, pp 1473–1488.
45. S.T. Alvi, M.N. Uddin, L. Islam, S. Ahamed. DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. *J. King Saud Univ. - Comput. Inf. Sci.* **2022**, 34 (9), 6855–6871.
46. P. Chinnasamy, P. Deepalakshmi. HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. *J. Ambient Intell. Humaniz. Comput.* **2022**, 13 (2), 1001–1019.
47. J. Ma. Blockchain Consensus Mechanism Based on Improved Distributed Consistency and Hash Entropy. *Sci. Program.* **2021**, 2021, 2030810.
48. A.O. Bang, U.P. Rao. A novel decentralized security architecture against sybil attack in RPL-based IoT networks: a focus on smart home use case. *J. Supercomput.* **2021**, 77 (12), 13703–13738.
49. Z. Yang, M. Li, R. Yang, F.R. Yu, Y. Zhang. Blockchain Sharding Strategy for Collaborative Computing Internet of Things Combining Dynamic Clustering and Deep Reinforcement Learning. In *ICC 2022 - IEEE International Conference on Communications*; IEEE, **2022**,137, 2786–2791.
50. R. Huang, X. Yang, P. Ajay. Consensus mechanism for software-defined blockchain in internet of things. *Internet Things Cyber-Physical Syst.* **2023**, 3, 52–60.
51. P. Prabha, K. Chatterjee. Design and implementation of hybrid consensus mechanism for IoT based healthcare system security. *Int. J. Inf. Technol.* **2022**, 14 (3), 1381–1396.
52. S. Meisami, M.B. Atashgah, M.R. Aref. Using Blockchain to Achieve Decentralized Privacy in IoT Healthcare. *Int. J. Cybern. Informatics* **2023**, 12 (2), 97–108.
53. S. López-Sorribes, J. Rius-Torrentó, F. Solsona-Tehàs. A Bibliometric Review of the Evolution of Blockchain Technologies. *Sensors*. **2023**, 6, 3167.
54. Y. Lamriji, M. Kasri, K. El Makkaoui, A. Beni-Hssane. A Comparative Study of Consensus Algorithms for Blockchain. *3rd Int. Conf. Innov. Res. Appl. Sci. Eng. Technol. (IRASET* **2023**, 1–8.