# Advances in Consortium Chain Scalability: A Review of the Practical Byzantine Fault Tolerance Consensus Algorithm

Nur Haliza Abdul Wahab[1], Zhang Dayong[2], Juniardi Nur Fadila[3], Keng Yinn Wong[4]
Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia[1, 2, 3]
Faculty of Mechanical, Universiti Teknologi Malaysia, Johor Bahru, Malaysia[4]

***Abstract*—Blockchain technology, renowned for its decentralized, immutable, and transparent features, offers a reliable framework for trust in distributed systems. The growing popularity of consortium blockchains, which include public, private, hybrid, and consortium chains, stems from their balance of privacy and collaboration. A significant challenge in these systems is the scalability of consensus mechanisms, particularly when employing the Practical Byzantine Fault Tolerance (PBFT) algorithm. This review focuses on enhancing PBFT's scalability, a critical factor in the effectiveness of consortium chains. Innovations such as Boneh–Lynn–Shacham (BLS) signatures and Verifiable Random Functions (VRF) are highlighted for their ability to reduce algorithmic complexity and increase transaction throughput. The discussion extends to real-world applications, particularly in platforms like Hyperledger Fabric, showcasing the practical benefits of these advancements. This paper provides a concise overview of the latest methodologies that enhance the performance scalability of PBFT-based consortium chains, serving as a valuable resource for researchers and practitioners aiming to optimize these systems for high-performance demands.**

***Keywords*—Blockchain; Practical Byzantine Fault Tolerance (PBFT); consensus algorithm; cryptography**

## I. INTRODUCTION

A major worry in both academic and industrial circles in the Big Data era brought about by 5G, Artificial Intelligence (AI), and Internet of Things (IoT) breakthroughs is safeguarding human privacy and data security [1]. Traditional centralized data management solutions frequently fail, especially when it comes to large-scale applications because of flaws including data tampering concerns, single points of failure, and vulnerability to denial-of-service assaults [2].

Blockchain technology offers a novel approach to data security and privacy protection because of its decentralization, non-tamper ability, and openness, transparency, and traceability features. Public chains, private chains, hybrid, and consortium chains are some of its variants. Of these, consortium chains are becoming more and more popular since they are appropriate for enterprise-level applications and provide systems for identity management and controlled access [3].

Consensus is the foundation of blockchain technology and is essential to maintaining data consistency and integrity over a distributed network. In addition to being the cornerstone of blockchain design, the consensus mechanism plays a crucial role in defining the network's ability to handle transactions and grow efficiently [4]. Due to its higher performance and energy efficiency, the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm is frequently chosen in consortium chains, which are being adopted more and more for their industry-specific applications over the more energy-intensive Proof of Work (PoW) used in public chains.

Even while PBFT is advantageous in consortium chains, there are several drawbacks, especially with regard to performance scalability [5]. The system experiences a decrease in performance as the network grows and the number of blocks rises. This is because creating new blocks takes longer and puts more strain on node storage capacity [6]. Although there are many facets to these difficulties, including network, storage, and performance scalability, this research focuses on the crucial component of performance scalability, which is essential for consortium chain throughput and responsiveness [7].

This paper summarizes and evaluates the literature on the performance scalability of PBFT-based consortium chains, with a focus on novel approaches that have been developed to overcome the bottlenecks in performance. In particular, we investigate the use of Boneh–Lynn–Shacham (BLS) signatures and Verifiable Random Functions (VRF) [8], [9], which are noteworthy developments in lowering algorithmic complexity and speeding up transaction processing [10].

In order to gain a thorough understanding of the scalability solution landscape, this review will conduct a systematic literature review (SLR) of relevant research, focusing on papers that overlap VRF, PBFT, BLS cryptography, and consortium blockchains. Prominent databases such as IEEE Xplore, SpringerLink, and Elsevier's ScienceDirect will be searched by the SLR in order to compile and analyze research that has been published between 2018 and 2023 [11]. This temporal window provides a current snapshot of the state of performance scalability in consortium chains by capturing the latest developments and conversations in the area.

Through the examination of various sources, the review seeks to condense a clear picture of the approaches, difficulties, and innovations that are now being faced in the field of consortium blockchain scalability [12]. The goal is to provide a condensed body of knowledge that will help practitioners and researchers comprehend the evolution of scalability

optimizations and their useful applications in the context of PBFT.

## II. Literature Review

The development and introduction of Bitcoin, which was first made public in 2008 by an individual or group going by the pseudonym Satoshi Nakamoto, is credited with the invention of blockchain technology [13]. The first decentralized digital currency, Bitcoin, was launched in Nakamoto's whitepaper, "Bitcoin: A Peer-to-Peer Electronic Cash System," which also established the framework for blockchain technology [14].

The Origin of Bitcoin and the Underlying Blockchain Idea start by using a peer-to-peer network. Bitcoin offered the first workable solution to the issue of double-spending in digital money [15], [16]. Its distributed ledger, or blockchain, which records every transaction over a network of computers without the need for a central authority, is the main innovation [17], [18]. The decentralized structure of blockchain guaranteed data security, integrity, and transparency [19].

The next big development in blockchain technology, commonly known as Blockchain 2.0, was launched in 2015 with the introduction of Ethereum by Vitalik Buterin and associates [20], [21]. Ethereum extended the usage of blockchain technology to incorporate "smart contracts," which are self-executing contracts with the contents of the agreement between the buyer and seller explicitly encoded into code, in contrast to Bitcoin's focus on financial transactions[22], [23]. This breakthrough made it possible for blockchain to be used for purposes other than cryptocurrency, allowing for the development of decentralized application (DApp)[24], [25], [26]. The third development in blockchain technology is the division of the technology into four primary categories: public, private, hybrid and consortium chains [27].

Following the introduction of Ethereum and smart contracts, the focus in the blockchain community shifted to consensus mechanism optimization for various network architectures [28], [29]. Of them, PBFT has become a prominent algorithm for consortium chains networks that are more open than private networks but still need a more regulated environment than public blockchains[30], [31], [32].

Consensus algorithm development in blockchain technology is essential to maintaining dependability and confidence in decentralized systems [4], [33], [34]. There are two types of these algorithms: non-Byzantine fault-tolerant and Byzantine fault-tolerant (BFT). Byzantine defects, or hostile components present in the system, do not prevent consensus in BFT algorithms [35].

Fig. 1 in this research shows the evolution and relationships between various algorithms in a chronological order. An arrow from algorithm A to algorithm B, for example, indicates that algorithm A influences algorithm B. Arrows from both point to an algorithm like C, which is a hybrid algorithm inspired by both A and B.

The inception of consensus algorithms can be traced back to non-BFT protocols such as Viewstamped Replication and Paxos. The Proof of Work (PoW) algorithm, which was first established with the introduction of Bitcoin, completely changed the way consensus was reached in a trustless setting. But because PoW requires a lot of energy, substitutes like Proof of Stake (PoS) and its variations were created in an effort to find consensus procedures that use less energy [36].

The Practical Byzantine Fault Tolerance (PBFT) algorithm has had a major impact on the Byzantine fault-tolerant category. It has sparked additional innovations like Tendermint and Honey Badger, which provide enhanced efficiency and adaptability in a range of network conditions.

PBFT is advantageous to consortium chains because of its low latency and finality of transactions, which are critical for business applications where immutability and transaction speed are crucial. Since PBFT presupposes that a certain amount of trust is built between nodes, a feature intrinsic to the consortium model, consortium chains, as opposed to public chains, might use it to expedite their consensus process [37].

Although PBFT offers consortium chains a dependable consensus method, as the network expands, its scalability becomes problematic. A variety of PBFT improvements are suggested in the literature in order to address these scaling issues. These include lowering the overhead necessary to obtain consensus, strengthening the algorithm's resistance to node failure, and optimizing the communication complexity [7].

The focus of current scientific debate on PBFT is on enhancing its performance scalability in order to accommodate consortium chains' growing requirements. A number of changes and implementations have been suggested in recent research to address the shortcomings of PBFT. These include the use of sharding strategies, sophisticated cryptographic techniques like BLS signatures and VRF, and the utilization of trusted execution environments to improve the consensus process's throughput and effectiveness [38].

Essentially, PBFT has proven to be the best consensus method for consortium chains, fitting their requirement for a well-balanced approach to efficiency and trust. By showcasing the advancements that are propelling this subject forward, this section of the literature review lays the groundwork for a more in-depth analysis of the performance scalability of PBFT within consortium chains [6].

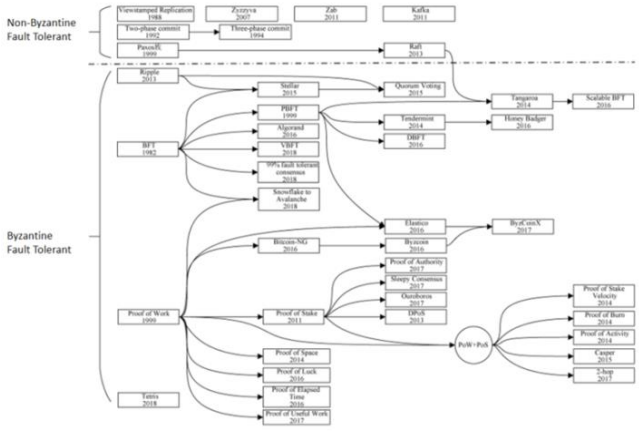


Fig. 1. Summary of consensus mechanism.

### A. Fundamentals of Consortium Chains

Consortium chains are an example of a hybrid blockchain technology that combines public blockchain transparency with the controlled governance of private networks. These networks, which are run by a coalition of organizations, provide a collaborative setting where a limited number of pre-approved nodes are in charge of governance. The customized governance provided by this arrangement satisfies the unique requirements of the involved companies.

Consortium chains, which are ideal for sectors needing compliance and secrecy, combine data protection and integrity in a way that is selectively transparent [39]. Because there are fewer nodes, consensus and transaction processes proceed more quickly, improving scalability and making these chains perfect for industry-specific applications [40].

Consortium chains, while more centralized than public blockchains, provide security by reducing the possibility of single points of failure through the distribution of trust across verified members. Usually, they use energy-efficient consensus algorithms like PBFT, which give fast consensus at a lower cost than Proof of Work [31].

Consortium chains, a growing trend in industries like finance, healthcare, and supply chain management, combine privacy, trust, and cooperative efficiency. Their architecture demonstrates a dedication to establishing safe, expandable blockchain networks for inter-organizational cooperation.

As depicted in Fig. 2, the volume of research pertaining to consortium chains has seen a significant increase from 2020 to 2023. This upward trend continues into 2024, with early access articles on the subject already available. This suggests that the field of consortium chain research remains ripe with opportunities for exploration and innovation.

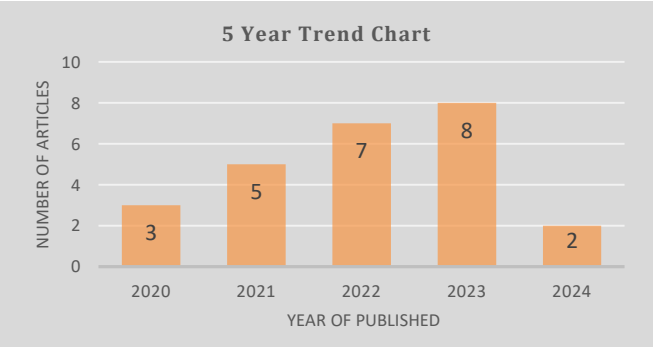


Fig. 2. Latest five years article trends of consortium chains topic studies.

This surge in research activity aligns with the publishing trends observed among researchers. As elucidated in Fig. 3, the Institute of Electrical and Electronics Engineers (IEEE) remains the most popular publisher among researchers in this field. Elsevier follows closely, contributing a substantial number of articles over the past five years.

Despite their efforts, Taylor & Francis and Wiley have yet to surpass Springer in terms of the number of published articles. This indicates a competitive landscape among publishers, with Springer maintaining a strong presence in the dissemination of consortium chain research. This dynamic interplay between researchers and publishers underscores the vibrancy and ongoing evolution of the field.

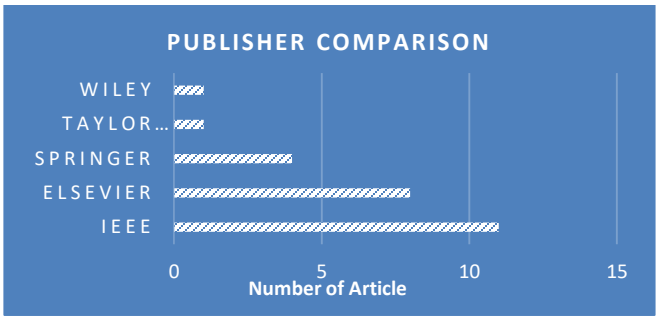


Fig. 3. Publisher destination for consortium chain topic studies.

Upon further analysis, TABLE Iprovides a comparative study of the articles across all databases, categorized into three main criteria: consensus, security, and improvement. The distribution of articles is shown in the matrix, with 41 articles focusing on consensus, 59 on security, and 54 on improvement. Additionally, there are overlaps where articles address multiple criteria, such as 19 articles covering both consensus and security, 12 articles on consensus and improvement, and 24 articles on security and improvement. This matrix highlights the diverse focus areas and intersections within the research landscape.

TABLE I. MATRIX TABLE OF RECORD FINDING BASED ON TOPIC

| | Consensus | Security | Improvement |
|---|---|---|---|
| Consensus | 41 | | |
| Security | 19 | 59 | |
| Improvement | 12 | 24 | 54 |

Moreover, on the TABLE IIoutlines several methods for managing consortium chains, highlighting their respective advantages and disadvantages. These methods include consensus algorithms, encryption mechanisms, access control techniques, and trust incentive models. Each method offers unique benefits, such as reducing consensus delays, improving encryption efficiency, and enhancing trust in federated learning. However, they also come with specific challenges, such as low consensus efficiency, lack of fine-grained access control, and high energy consumption. This comparative analysis provides a comprehensive overview of the strengths and limitations of each approach, aiding in the selection of the most suitable method for managing consortium chains.

There's a focus on advanced consensus algorithms for improved blockchain network efficiency, as seen in the work of [41]. Enhanced encryption mechanisms and access control methods are being utilized for better data security, as demonstrated by study [39]. The importance of decentralization and fairness in the consensus process is highlighted by [42] research. Trust incentive consensus methods, like the one proposed by [43], are gaining traction to boost trust in federated learning. Lastly, the emergence of cross-chain communication mechanisms, as proposed by study [40], simplifies node topology for dynamic interaction, facilitating safe and autonomous sharing of patient records.

TABLE II. METHODS ON CONSORTIUM CHAIN ARTICLES

| Method | Advantages | Disadvantages | Category |
|---|---|---|---|
| Consensus algorithm based on PBFT [41] | Reduces consensus delay and communication times between nodes. | Inability to dynamically join nodes, low consensus efficiency, primary master node selection challenges. | Consensus |
| Improved Paillier homomorphic encryption [39] | Reduces overall encryption and decryption time. | Lack of data ownership and fine-grained access control, lack of transparency and auditability. | Encryption |
| CP-ABE for access control [39] | Adaptive for storing massive data. | Time-consuming decryption (about 2 seconds). | Decryption |
| Voting-based decentralized consensus algorithm [42] | Faster consensus process, better user fairness, negligible energy cost, adequate security. | Ultrahigh energy consumption, time inefficiency, low transaction throughput. | Consensus |
| Trust rewards and punishments method [43] | Improves trust perception in federated learning. | Limitations in main node's misbehavior or fault tolerance. | Consensus |
| Cross-chain communication mechanism [40] | Safe and autonomous sharing of patient records within milliseconds. | No specific limitations mentioned. | Sharing |

The comparative analysis reveals that while each method offers unique advantages, they also come with specific limitations that need to be addressed. For instance, consensus algorithms like PBFT and voting-based methods improve efficiency and fairness but face scalability and energy consumption issues. Encryption methods like Improved Paillier and CP-ABE enhance performance but lack fine-grained control and transparency. Trust-based methods and cross-chain mechanisms show promise in improving trust and interoperability but may face challenges in fault tolerance and integration.

### *B. PBFT Consensus Mechanism and its Evolution*

Miguel Castro and Barbara Liskov created the PBFT consensus algorithm in 1999, and it is a key component of consortium blockchain networks' consensus procedures. PBFT is a distributed system reliability technique that tackles the problem of Byzantine faults, which are caused by some nodes in the network acting in an unpredictable manner [32]. It uses a multi-phase communication protocol that involves multiple rounds of node contact to achieve system consistency. The request, pre-prepare, prepare, and commit phases of this procedure enable the network to come to a consensus even when there are malicious or malfunctioning nodes present—as long as they make up no more than one-third of the total.

When compared to the PoW algorithm, PBFT is more efficient and uses less resources, which is why consortium chains prefer it. Because of its deterministic structure, transactions are completed quickly after a single consensus round, obviating the need for several probabilistic rounds that are common to other algorithms [44].

RBFT and BFT-SMaRt are two examples of the many improvements made to PBFT over time that have improved its resource management and scalability. These improvements are designed to support the growing complexity and scale of contemporary distributed networks while preserving the robustness of PBFT [45].

Scalability, node selection optimization, communication efficiency, and data management have all been continuously prioritized in PBFT's evolution in order to better support larger and more complicated consortium chain applications. Since its inception, this algorithm has developed into a commonly used mechanism in consortium chains because of its ability to balance performance, efficiency, and fault tolerance. This section examines the development of PBFT from theory to application, highlighting its vital role in consortium chains' expansion and success [32].

Fig. 4 depicts a clear upward trend in the research on this topic over the past five years. This suggests a growing interest in PBFT within the academic community, reflecting its increasing relevance in the field of distributed systems. The sustained growth in research output underscores the importance and potential of PBFT in advancing our understanding of Byzantine fault tolerance in practical applications. This trend is expected to continue, fostering further innovation and exploration in this area.

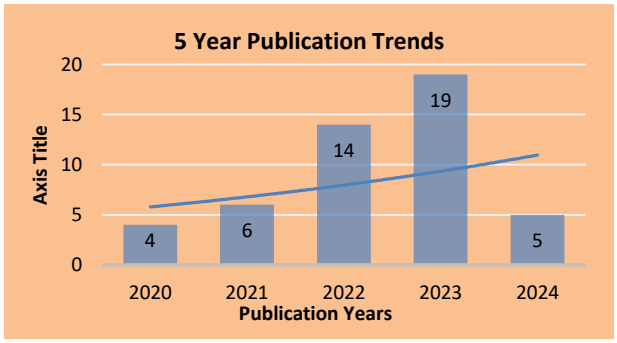


Fig. 4. Latest five years article trends of PBFT topic studies.

Furthermore, as illustrated in Fig. 5, the distribution of studies on PBFT is predominantly concentrated among three major publishers: IEEE, Elsevier, and Springer. These publishers have been instrumental in disseminating a significant volume of research on this topic. Interestingly, there appears to be a conspicuous absence of PBFT studies in both Wiley and Taylor & Francis, indicating a potential gap in their publication portfolio.

Further analysis on the PBFT articles which is lead to comparison TABLE III, we find diverse methods being explored. [7] and [41] both focus on PBFT consensus mechanisms, with the former targeting large systems and the latter aiming to reduce consensus delay. [46] integrate cryptographic primitives with Byzantine fault tolerance, while [47] use a PoQF consensus algorithm for VEC networks. The research in [48] propose a blockchain-based method for medication traceability. Each study has its unique advantages and challenges, contributing to the evolving research landscape. The upward trend in research output suggests a promising future for these methods in practical applications.


Fig. 5. Publisher destination spreads for PBFT studies.

TABLE III. STUDIES COMPARISON IN PBFT TOPIC

| Method | Advantages | Disadvantages |
|---|---|---|
| Scalable multi-layer PBFT [7] | Validated security threshold, effective in simulations. | Poor node scalability, suitable for small networks. |
| Consensus algorithm based on PBFT [41] | Reduces consensus delay and communication times. | Inability to dynamically join nodes, low consensus efficiency, primary master node selection challenges. |
| Integration of cryptographic primitives and PBFT [46] | Removes transaction fees and mining rewards for better performance. | Lacks conflicting properties like anonymity and regulation. |
| PoQF consensus for VEC networks [47] | Reduces validation failure by 11%, faster message validation. | PoS favors nodes with higher stakes, PoET lacks security against malicious nodes. |
| Blockchain-based medication anti-counterfeiting [48] | Ensures transparency, openness, and full record of medication circulation. | No specific limitations mentioned. |

Regarding to the study comparison, the Scalable multi-layer PBFT method demonstrates a validated security threshold and effectiveness in simulations, making it a reliable choice for small networks. However, its poor node scalability limits its applicability in larger systems, highlighting a significant drawback for broader adoption. The Consensus algorithm based on PBFT effectively reduces consensus delay and communication times, which is crucial for enhancing network efficiency. Nevertheless, its inability to dynamically join nodes, coupled with low consensus efficiency and challenges in primary master node selection, restricts its flexibility and scalability in dynamic environments.

The Integration of cryptographic primitives and PBFT offers improved performance by eliminating transaction fees and mining rewards. This integration enhances the overall efficiency of the blockchain system. However, it lacks conflicting properties such as anonymity and regulation, which are essential for certain applications requiring privacy and compliance. The PoQF consensus for VEC networks method stands out by reducing validation failure by 11% and providing faster message validation compared to other consensus algorithms like PoS and PoET. Despite these advantages, it faces challenges such as PoS favoring nodes with higher stakes and PoET's vulnerability to malicious nodes, which can compromise the network's security and fairness.

Lastly, the Blockchain-based medication anti-counterfeiting method ensures transparency, openness, and a comprehensive record of medication circulation, which is vital for maintaining trust and integrity in the pharmaceutical supply chain. However, the absence of specific limitations in the provided context suggests that further scrutiny is needed to identify potential challenges in practical implementation. Overall, while each method offers unique strengths, they also come with specific limitations that need to be addressed. Future research should focus on developing hybrid approaches that combine the strengths of these methods while mitigating their weaknesses to create more robust, scalable, and secure blockchain systems.

## III. PERFORMANCE SCALABILITY

Consortium chains, which provide a sophisticated architecture al solution that balances completely private and fully public networks, have becoming increasingly popular in the blockchain space. Nevertheless, a crucial and urgent issue facing these consortium networks is performance scalability, particularly for those depending on the PBFT consensus algorithm[11], [32].

The way consortium chains handle transactions is at the core of the problem. Their use of conventional transaction processing techniques, which are mainly defined by serial verification and transaction storing, is intrinsically constrained. These traditional methods place fundamental limitations on the blockchain system's ability to effectively manage an increasing number of transactions[49]. These restrictions represent a major bottleneck in the context of PBFT-based consortium chains, which priorities fast and dependable consensus.

As the need for high-performance applications keeps growing, the performance scalability issue gets worse. Consortium chains are used in a number of sectors, including supply chain management, healthcare, and banking, where effective transaction processing is critical. These industries need blockchain systems that can process a large number of transactions efficiently and rapidly[45].

The emphasis is now being placed on more sophisticated and creative approaches rather than the traditional block scaling methods, which have drawbacks. Improving consensus algorithms has been a vital path to improving consortium chain performance. Throughput and scalability have grown as a result of the PBFT consensus process being streamlined by innovations like Tendermint and Honey Badger BFT.

Moreover, using cryptography methods like VRF and BLS signatures is another interesting way to address the performance scalability issue. These cryptographic techniques provide a workable way to increase transaction throughput while preserving the required degree of privacy and confidentiality, in addition to strengthening the security and integrity of consortium chains. Several related research on performance scalability optimization schemes is shown in Table IV.

TABLE IV. SUMMARY OF PERFORMANCE SCALABILITY OPTIMISATION SCHEMES

| Optimization Scheme | Description | Application | Advantages | Disadvantages |
|---|---|---|---|---|
| **Traditional Block Scaling Methods** | Serial verification and transaction storing. | Initial stages of consortium chains. | Simple to implement and understand. | Limited scalability; ineffective for increasing transactions. |
| **Consensus Algorithm Improvements** | Enhancements like Tendermint and Honey Badger BFT. | Modern consortium chains. | Improved performance and scalability; handles larger transaction volumes. | Complex to implement; higher computational resources needed. |
| **Cryptography Methods (VRF and BLS signatures)** | Techniques to increase throughput while preserving privacy. | Various sectors using consortium chains. | Increases transaction throughput; maintains privacy and confidentiality. | Requires advanced cryptographic knowledge; potential speed-security trade-off. |

Regarding to that comparison table, Traditional block scaling methods, while simple to implement and understand, suffer from limited scalability and inefficiency in handling increasing transaction volumes. In contrast, consensus algorithm improvements, such as Tendermint and Honey Badger BFT, offer enhanced performance and scalability, making them suitable for modern consortium chains. However, these improvements come with increased complexity and higher computational resource requirements. Cryptographic methods, including VRF and BLS signatures, provide significant advantages in transaction throughput and privacy preservation, making them valuable in various sectors. Nevertheless, these methods demand advanced cryptographic knowledge and may involve trade-offs between speed and security. Overall, while each optimization scheme offers unique benefits, their limitations must be carefully considered to ensure effective and scalable consortium chain management.

This chapter is essentially an in-depth investigation of the various performance scalability problems that consortium chains, particularly ones that depend on PBFT face. It explores a number of potential solutions, such as improvements in consensus algorithms and the thoughtful fusion of cryptographic methods like as VRF and BLS. The ultimate goal is to give a thorough overview of the strategies used to solve the crucial performance scalability issue, opening the door for the creation of consortium blockchain networks that are both highly scalable and effective, satisfying the requirements of contemporary high-performance applications.

### *A. PBFT-Based Performance Scalability in Consortium Chains*

One major difficulty in the field of blockchain technology is the performance scalability of consortium chains, especially those that use the Practical Byzantine Fault Tolerance (PBFT) consensus method [32]. Consortium chains present a promising hybrid solution that combines the openness of public blockchains with the regulatory advantages of private networks; nevertheless, their performance scalability is severely constrained [50], [51]. The main issue with performance scalability in consortium chains is presented in this section, with particular attention paid to the application of the PBFT consensus algorithm.

*1) The challenge of performance scalability:* Consortium chains are well-suited for various applications, including supply chain management, finance, and healthcare, due to their collaborative nature among a limited number of organizations. However, as the demand for high-performance and scalable solutions grows, the scalability of consortium chains becomes a significant challenge. This issue is particularly pronounced in systems relying on PBFT consensus mechanisms. The core issue lies in the traditional techniques for transaction processing used by blockchain systems. The process of serial verification and storage of transactions inherently limits transaction throughput. This bottleneck is especially problematic for PBFT-based consortium chains, where achieving quick and reliable consensus is crucial. As the number of nodes increases, the communication overhead and consensus delay also rise, leading to decreased performance and scalability.

*2) How consortium chains are affected?:* Consortium chains are perfect for a variety of use cases, such as supply chain management, finance, and healthcare, since they are made to encourage collaboration among a small number of organizations, unfortunately, the consequences of performance scalability limits for consortium chains are extensive.

*a) Transaction throughput:* Consortium chains' ability to effectively handle a large number of transactions is limited by the traditional transaction processing techniques. The inability to meet the expectations of industries seeking simultaneous and speedy transaction validation is caused by this bottleneck.

*b) Latency:* Prolonged delays in transaction processing lead to higher latency, which affects consortium chains' ability to respond quickly. This is especially important for industries where instantaneous decision-making and data accessibility are crucial.

*c) Limitations on scalability:* The extensive use of consortium chains depends critically on scalability. Consortium chains run the danger of being unsuitable for large-scale enterprise applications if performance scalability is not addressed.

*3) How to Address the Issues?:* To address the scalability challenges in consortium chains, several improvements and alternative approaches have been proposed. Enhanced versions of PBFT, such as tPBFT and CBFT, introduce mechanisms like trust-based scoring and grouping of nodes to reduce communication overhead and improve consensus efficiency. These methods show promise in increasing the scalability of PBFT-based systems by dynamically adjusting the list of consensus nodes and simplifying the consensus process. Another approach involves integrating cryptographic primitives and other consensus algorithms to balance performance and security. For instance, combining PBFT with techniques like sharding or layer-2 solutions can help

distribute the consensus workload and improve scalability without compromising security.

While PBFT offers robust fault tolerance and deterministic finality, its scalability limitations pose significant challenges for consortium chains. Addressing these challenges requires innovative approaches that enhance the consensus process and reduce communication overhead. By adopting hybrid consensus mechanisms and advanced cryptographic techniques, it is possible to develop more scalable and efficient consortium chains that meet the growing demands of various applications. This comprehensive approach will ensure that the strengths of each method are maximized while mitigating their limitations, leading to more efficient and secure blockchain applications.

Creative solutions are essential for overcoming the performance scalability difficulties in consortium chains. This analysis examines numerous strategies and developments aimed at mitigating these restrictions. The goal of the review is to illuminate the path towards more effective and scalable consortium blockchain networks by examining advancements in consensus algorithms, the incorporation of cryptographic techniques such as Verifiable Random Function (VRF) and Boneh-Lynn-Shacham (BLS) signatures, and other cutting-edge tactics. In the following sections, we explore these approaches and how they can improve performance scalability in consortium chains. By conducting a thorough assessment of pertinent studies published between 2018 and 2023, we aim to shed light on the evolving scalability of consortium chains and its implications for the blockchain sector.

### B. Utilizing Boney-Lynn-Shacham (BLS) Signatures for Enhanced Consensus Efficiency

In the field of blockchain technology, BLS signatures have become a potent cryptographic tool with a wide range of uses. BLS signatures, which were first proposed by Boneh, Lynn, and Shacham in 2004 and then substantially improved in 2018, provide a unique method for aggregating signatures and improve the security and efficiency of consensus algorithms in consortium blockchains [12], [52], [53].

Although consortium blockchains are renowned for their tightly managed governance, they have scalability issues with the effectiveness of their consensus processes. Although reliable, the conventional PBFT consensus mechanism can be computationally and communication-intensive, which limits its scalability as blockchain networks get bigger and more complicated [54].

When it comes to consensus algorithms like PBFT, researchers and developers have realized that BLS signatures can help solve some of the efficiency issues that consortium blockchains face. The literature has examined the following crucial elements:

*1) Simplifying Consensus via BLS:* In order to streamline the consensus process and lower computational overhead and communication complexity, BLS signatures are used. By using signature aggregation techniques, nodes can reduce the number of messages they exchange with one another during consensus by combining many individual signatures into a single aggregated signature.

*2) Improved scalability:* Convergence algorithms become more scalable when BLS signatures are integrated. Consortium blockchain technology facilitates the processing of transactions more efficiently and may support larger networks due to the decrease in computer resources and communication overhead.

*3) Security points to remember:* The security ramifications of using BLS signatures are also covered in the literature. The resilience of BLS signature methods against different types of attacks and their capacity to preserve the validity and integrity of transactions are examined.

*4) Uses not limited to consensus:* Beyond consensus methods, BLS signatures are used in a variety of consortium blockchain network applications, including as identity management, access control, and privacy-preserving transactions. Scholars have investigated how BLS signatures might be used to improve consortium blockchain security and functionality in general.

Particularly in the context of PBFT, the literature on BLS signatures in consortium blockchains emphasizes their potential to solve efficiency issues and enhance the scalability of consensus algorithms. More investigation into sophisticated cryptographic methods and their incorporation into consortium blockchains is anticipated as blockchain technology develops, opening the door to more effective and secure decentralized networks. A promising first step towards accomplishing these goals and enhancing consortium blockchain capabilities is the implementation of BLS signatures.

Several articles found on the database that related to utilize of BLS Signature can be seen on TABLE V

TABLE V. RELATED TO HIGH-CITED STUDIES BASED ON BLS SIGNATURE KEYWORD

| References | Key Findings | Advantages | Disadvantages |
|---|---|---|---|
| [55] | The paper introduces the notion of outsourced proofs of retrievability (OPOR), where users can task an external auditor to perform and verify proofs of retrievability (POR) with the cloud provider. | The OPOR setting provides a solution to security risks not covered by existing POR security models. | The paper does not provide a comprehensive analysis of potential attacks or countermeasures. |
| [56], [57] | The paper presents LDuAP, a lightweight dual auditing protocol that verifies data integrity in cloud storage servers. It combines public and private auditing schemes to improve the authenticity of the integrity results. | LDuAP reduces the size of the signature by 50% and subsequently reduces the overhead of the entire auditing scheme. | The paper does not discuss the potential impact of compromised auditors. |
| [8], [58] | The paper proposes a cryptographic framework for contact tracing and provides a | The system provides comprehensive privacy | The paper does not discuss the potential impact of environmental |

| | | | |
|---|---|---|---|
| | construction based on public key rerandomizable BLS signatures. It uses environmental factors to filter out results outside estimated effective transmission distance. | protection and takes airborne transmission into consideration. | changes on the system's performance. |
| [8], [54], [58], [59], [60] | The paper presents a chain-based unique signature scheme where each unique signature is composed of n BLS signatures computed sequentially like a blockchain. | The proposed scheme achieves optimal tightness and significantly improves on previous reduction loss. | The paper does not discuss potential attacks or countermeasures. |
| [8], [54], [57] | The paper presents a dynamic provable data possession scheme for secure cloud data auditing. The scheme leverages BLS signatures and RMHT to support batch auditing and then optimizes batch auditing scenarios with four algorithms to support efficient batch updates. | The proposed scheme supports efficient batch updates and reduces the overhead of the entire auditing scheme. | The paper does not discuss the potential impact of compromised auditors. |
| [21], [61] | The paper presents a novel robust solution for key management, message encryption, and authentication, offering enhanced security for 5G-V2X communication. | The protocol achieves a high level of security and incorporates bilinear pairing, and AES encryption. | The paper does not discuss potential attacks or countermeasures. |
| [8], [58], [62] | The paper proposes a modification of BLS signatures with an additive key split augmented with a refresh technique. | The proposed scheme protects against a powerful adversary that can control distinct HSMs in different signing sessions. | The paper does not discuss potential attacks or countermeasures. |
| [21], [60] | The paper proposes an authentication mechanism that allows a Seed OppNet to process pieces of information effectively and efficiently. | The proposed scheme is secure against the rogue pubic key, tapping, forgery, replay, and man-in-the-middle attacks. | The paper does not discuss potential attacks or countermeasures. |

### *C. Verifiable Random Function (VRF) for Enhancing Consortium Chain Performance*

Performance scalability in consortium chains is still a major concern. These blockchain networks, which are overseen by a small number of institutions, put efficiency, security, and trust first. Because of its effectiveness and speed at reaching consensus, the Practical Byzantine Fault Tolerance (PBFT) consensus method is frequently chosen in consortium chains. Nevertheless, despite these benefits, consortium chains—PBFT-based included face constraints in their performance that limit their capacity to manage an increasing number of players and transactions [32], [63].

The blockchain's transaction processing is at the centre of the performance scalability problem for consortium chains. Conventional methods for storing and verifying transactions restrict these systems' capabilities. This problem is more apparent in PBFT-based consortium chains, where prompt and trustworthy node agreement is crucial. Researchers and developers have turned away from traditional block scaling techniques in favour of creative approaches meant to improve performance in order to overcome these constraints [63].

Consensus algorithm optimization is one of the key areas to increase consortium chain performance. Tendermint and Honey Badger BFT are two examples of notable inventions that simplify the PBFT consensus procedure. These developments improve consortium chains' overall scalability in addition to increasing their throughput. These optimizations assist consortium chains satisfy the requirements of high-performance applications by lowering the computational cost of the consensus procedure.

Still, more than only consensus algorithms are involved in better performance. The efficiency of consortium chains has been significantly improved by the application of cryptographic techniques [11]. Verifiable Random Functions (VRF) are one of these methods that stands out as a potentially useful approach.

Fundamentally, VRF presents a new way to confirm the leader node in the PBFT consensus procedure. It accomplishes this by using a predetermined set of criteria to start the VRF process, which produces a cryptographic proof and a random integer. This number is then compared to a predefined threshold, which is ensured to be unique and unchangeable [32], [64], [65].

The value of VRF is found in its capacity to improve leader node election in a way that is both highly secure and unpredictable. Using VRF, the top nodes in the consortium chain with the highest trust value calculate random numbers, and the node with the highest value is named the leader. This strategy guarantees equity and lessens the possibility of manipulation or collaboration.

Using VRF in consortium chains has a number of noteworthy benefits. Above all, it strengthens the overall reliability of the PBFT consensus process by improving the security and randomness of leader node selection. Moreover, it adds a level of unpredictability that reduces the possibility of predictability, which bad actors could take advantage of.

In summary, Verifiable Random Functions (VRFs) present a promising avenue for enhancing the speed of consortium chains, especially those employing the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm. By introducing an additional layer of security and randomization to the consensus process, VRFs alter the selection mechanism for leader nodes, thereby better catering to the demands of high-performance applications. This discussion delves into the role of VRFs in augmenting the scalability and efficiency of consortium chains, a critical aspect of performance scalability

within this blockchain architecture. TABLE VIprovides a comprehensive overview of several studies that have incorporated VRFs as their foundational methodology.

TABLE VI. TOP FIVE HIGH CITED ARTICLE ABOUT VRF

| Author(s) | Article Title | Key Findings | Results |
|---|---|---|---|
| [66] | A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things | The paper introduces a novel bidirectional-linked blockchain (BLB) using chameleon hash functions to defeat double-spend attacks, long-range attacks, and eclipse attacks1. | The proposed blockchain consensus algorithm utilizes a verifiable random function (VRF) to select the third-party auditor committee (TPAC) which performs contract verification1. |
| [42] | Voting-Based Decentralized Consensus Design for Improving the Efficiency and Security of Consortium Blockchain | The paper introduces a voting-based decentralized consensus (VDC) algorithm for consortium blockchain to enhance the performance of blockchain platforms2. | The proposed blockchain consensus algorithm utilizes a verifiable random function (VRF) to select the third-party auditor committee (TPAC) which performs contract verification2. |
| [67] | Deep Video Prediction Network-based Inter-Frame Coding in HEVC | The paper proposes a novel Convolutional Neural Network (CNN) based video coding technique using a video prediction network (VPN) to support enhanced motion prediction in High Efficiency Video Coding (HEVC)3. | The proposed VPN uses two sub-VPN architectures in cascade to predict the current frame in the same time instance3. |
| [68] | Blockchain-based random auditor committee for integrity verification | The paper proposes a blockchain-based random auditor committee to replace the fixed TPAs for the integrity verification4. | The proposed blockchain consensus algorithm utilizes a verifiable random function (VRF) to select the third-party auditor committee (TPAC) which performs contract verification4. |
| [69] | A modified teaching learning metaheuristic algorithm with opposite-based learning for permutation flow-shop scheduling problem | The paper proposes a modified Teaching-Learning-Based Optimization with Opposite-Based-Learning algorithm to solve the Permutation Flow-Shop-Scheduling Problem with the purpose of minimizing the makespan5. | The proposed algorithm outperformed over five well-known datasets such as Carlier, Reeves, Heller, Taillards and VRF benchmark test functions, compared to other metaheuristic algorithms5. |

## IV. METHODOLOGY

In order to give a clear framework for the examination of scalability solutions inside consortium chains, this review paper outlines the scope of its research. It focuses on pertinent advances that have occurred between 2018 and 2023. The scope includes important areas of interest such as the use of BLS cryptography, the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm, and the Verifiable Random Function (VRF), especially in relation to consortium blockchains. Consortium chains are a unique architectural paradigm in the blockchain space, and this review's comprehension of their scaling issues and remedies is crucial. The review guarantees that it includes the most recent developments and conversations in the area by defining a temporal window that runs from 2018 to 2023. This gives readers an understanding of the state of scalability solutions inside consortium chains at the moment. This method helps to provide a thorough and current analysis by bringing the evaluation into line with the changing field of consortium chain scalability research.

### *A. Data Sources*

The use of relevant data sources is crucial for this in-depth analysis of consortium chains' scaling solutions in order to guarantee the accuracy and breadth of the study. In order to do this, reputable scholarly databases have been carefully selected to serve as the main sources for research articles. Notably, databases covering a wide range of academic articles related to consortium chains and blockchain technology, including IEEE Xplore, SpringerLink, and Elsevier's ScienceDirect, have been selected.

The assortment of research articles available in these well-chosen databases guarantees that the review will have access to a broad spectrum of scholarly sources. The choice to concentrate on reputable academic databases highlights the dedication to ensuring that the review is founded on reliable, authoritative, and peer-reviewed research. The robustness and dependability of the results offered in this journal paper are improved by this method.

With a focus on VRF, PBFT consensus algorithm, BLS cryptography, and their intersections, the review seeks to provide a thorough overview of the most recent advancements and discussions in the field of scalability solutions within consortium chains by utilizing these reliable data sources. The use of these databases strengthens the research's intellectual rigour and enhances its academic reputation.

### B. Search Strategy

The idea behind this search method is to be broad but targeted at the same time. The search makes sure that publications that are directly connected to the main consensus mechanism under examination are included by using keywords like "PBFT consensus algorithm" and "Practical Byzantine Fault Tolerance."

Furthermore, adding terms like "Verifiable Random Function (VRF)" and "BLS cryptography" will help you find research on advancements and approaches in cryptography, which are crucial for improving consortium chains' security and efficiency.

The crucial term "consortium blockchains" ensures that the consensus algorithm and scalability solutions are thoroughly investigated by extending the search to include all facets of consortium chains.

Last but not least, the term "scalability solutions" is a catch-all for studies that specifically tackle the scalability issues consortium chains encounter. This guarantees that the assessment takes into consideration the most recent advancements and conversations in this important field.

Boolean operators are used to make the search approach more adaptive and versatile. It enables the retrieval of research papers that precisely address the intersections of these keywords by allowing for precise keyword combinations. This methodical technique to finding significant literature guarantees that the evaluation is thorough, balanced, and includes the most relevant studies that are available in the chosen databases.

### C. Inclusion and Exclusion Criteria

To guarantee that the chosen research papers are in line with the main goals and parameters of the investigation, this evaluation utilizes a set of precisely outlined inclusion criteria. The following are included in the inclusion criteria:

- Pertinence to Scalability Solutions in Consortium Chains: Studies that specifically tackle scalability solutions in the framework of consortium chains are given careful consideration for publication. Verifiable Random Function (VRF), BLS cryptography, and the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm are the main areas of interest. Research papers that examine the connections between these subjects are especially appreciated.
- Publication Period: This study specifically takes into account research papers published between 2018 and 2023 in order to capture the most recent advancements and discussions in the field. This temporal window guarantees that the evaluation includes the most recent developments and discussions regarding the scalability of performance in consortium chains.

Exclusion criteria are used to weed out research papers that don't fit inside the designated chronological window or don't correspond with the listed research subjects in order to preserve the accuracy and significance of the review. The following are the exclusion requirements:

- Irrelevance to Specified Research Topics: Papers that are not relevant to the specified research topics—such as BLS cryptography, PBFT, VRF, and scalability solutions in consortium chains—will not be accepted. The review seeks to concentrate only on studies that directly advance our knowledge of performance scalability in this particular setting.
- Publication outside the Specified Time Frame: Studies released before 2018 or after 2023 are not included. This temporal restriction makes that the review is up to date and covers research done in the chosen period of time.

A thorough examination of the chosen literature is made possible by the rigorous use of these inclusion and exclusion criteria, which ensure that the review keeps a clear and focused focus on relevant research.

### D. Screening and Selection

The process of conducting a systematic literature review, or SLR, is designed to include stringent screening and selection phases. These steps are carefully crafted to find and select research articles that closely fit the specified parameters of the study. The following steps are sequential in the screening and selection process:

*1) First screening:* Review of Titles and Abstracts: Research paper titles and abstracts get a thorough examination at the first screening stage. The purpose of this preliminary evaluation is to determine how each publication relates to the defined scope of the research. Papers that demonstrate a strong fit with the research goals and thematic areas advance to the following phase.

*2) Whole-Text examination:* Detailed Evaluation: Selected papers move on to the full-text screening phase after the first screening. Here, every manuscript is carefully assessed in-depth to ensure that it is appropriate for inclusion in the review. This extensive evaluation includes a close look at the paper's methods, conclusions, and applicability to the designated study fields. Papers that fulfil the specified requirements for inclusion move on to the next round.

*3) Evaluation of quality:* Evaluating Credibility and Scholarliness: The chosen articles are subjected to a comprehensive analysis of their quality and rigour during the quality assessment step. The purpose of this evaluation is to guarantee that reliable, academic sources are included in the review. This grading takes into account various factors, including study technique, data integrity, citation sources, and general academic rigour. Merely those documents exhibiting an exceptional calibre of academic writing are kept for the thorough examination.

A careful and methodical approach characterizes the screening and selection procedure used in this SLR. This method is intended to preserve the review's integrity by making sure that the final selection of research papers closely follows the goals and scope of the study as defined. The study attempts to offer a thorough and academic analysis of the chosen

literature by utilising these stringent screening and selection phases.

### E. Data Extraction and Analysis

The methodical extraction of pertinent data is the following step after the selection of research articles is complete. This procedure is essential to extracting important data, conclusions, and insights from the chosen papers. The following are the essential phases in data extraction and analysis:

Data Extraction: Careful data extraction is applied to a selection of research papers. Research methods, empirical results, theoretical contributions, and noteworthy insights into the scalability of consortium chains are collected in a systematic manner, together with other pertinent material.

The gathered data is then rigorously subjected to thematic analysis. It is possible to identify recurring themes, new trends, and significant contributions in the field of consortium chain scalability with this analytical technique. A thorough grasp of the study landscape is attained by classifying and arranging the retrieved material into relevant themes.

### F. Synthesis and Review Composition

The review article's composition is carefully organized to provide a logical summary of the chosen research publications. This synthesis is structured around a number of important components, such as:

The review article's thematic organization is based on topics that were found during the examination of a few research publications. Every subject is associated with a particular facet of consortium chain scalability, allowing readers to effortlessly peruse related content.

Methodological Insights: This page offers an analysis of the approaches taken in the chosen studies. Offering a thorough overview of the research landscape, it emphasizes the different study approaches and methodologies utilized by academics to investigate consortium chain scalability.

Presenting the major conclusions and ramifications drawn from the chosen research publications is a primary goal of the review. The paper provides insightful information about the present status of performance scalability in consortium chains by summarizing important research findings.

### G. Conclusion

The evaluation concludes with a strong summary of the main lessons learned from the examined research publications. The following goals are fulfilled by the conclusion:

*1) Key takeaways synopsis:* It offers a succinct synopsis of the major discoveries and contributions that were emphasized during the evaluation. Readers can grasp the ideas obtained from the chosen research by reading this summary.

*2) Future implications:* The concluding section delves into the more extensive consequences of the examined studies for the scalability of consortium chains in the future. It explores possible ramifications for scholars, politicians, and industry practitioners.

*3) Future research directions:* The review indicates possible directions for further study and advancement in the area of consortium chain scalability. It advances the body of knowledge in the topic by highlighting areas that need more research.

With an emphasis on the PBFT consensus algorithm, the review paper seeks to offer a thorough and enlightening investigation of consortium chain scalability by adhering to this systematic methodology for data extraction, analysis, synthesis, and conclusion.

## V. Result and Discussion

Upon conducting an in-depth analysis of articles from various databases, several findings emerged concerning research topics in the consortium and chain area. As illustrated in Fig. 6, the discovered articles were predominantly disseminated as conference articles or proceedings (41%) and technical journal articles (59%).

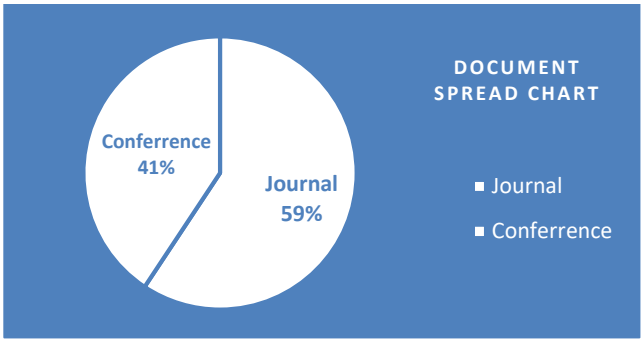


Fig. 6. Document type spreads of consortium + PBFT + VRF chain research.

These articles were distributed across a range of publisher databases as shown in Fig. 7, with IEEE being the most prominent publisher. Following IEEE, Elsevier and Springer occupy the middle tier. While Wiley and Taylor & Francis publishers constitute a smaller portion, they nonetheless contribute to the body of published articles on consortium and chain topics.

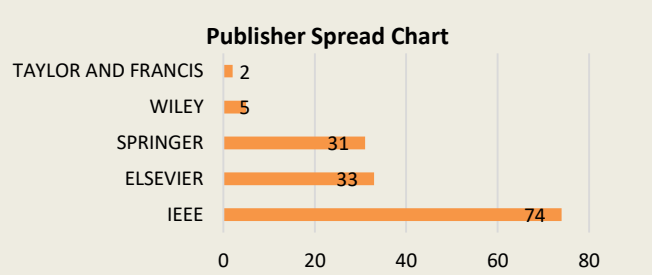


Fig. 7. Publisher spread of consortium + PBFT + VRF chain research.

The trend over the past decade reveals a consistent and significant increase in research related to consortium chains. Starting from 2014, there has been a steady rise in the number of studies published each year. The bar graph Fig. 8 underscores this growth, with the number of articles peaking at 313 in 2023. This surge not only highlights the escalating

interest in consortium chains but also indicates a substantial investment in its research and development.

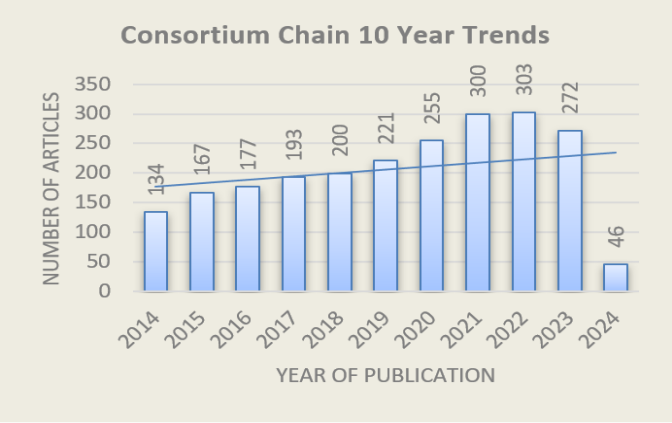


Fig. 8. Ten years trend of blockchain published articles.

The increasing trend suggests that consortium chains have become a significant area of focus in the contemporary technological landscape, particularly in the realm of blockchain technology. The continuous growth in research output also implies advancements in performance scalability and consensus algorithms, such as PBFT and BLS signatures, which are critical to the development and application of consortium chains. This trend is expected to continue as more technological innovations and applications emerge in the field.

The chart further illustrates in Fig. 9 that the research on this topic is not confined to a single domain but spans across multiple areas, reflecting its interdisciplinary nature. The areas include Engineering, Telecommunication, Automation and Control, Medical, Education, and Business. Engineering emerges as a dominant field in this distribution, signifying its substantial role and contribution. Telecommunication and Automation & Control follow closely, emphasizing the integration of advanced technologies and automated systems in the research landscape. The presence of Medical and Education sectors in the chart highlights the cross-disciplinary impact of the research, where innovations and findings are influencing healthcare and learning environments. The inclusion of Business underscores the commercial potential and economic implications associated with advancements in this field. This diverse spread of research areas indicates the broad applicability and transformative potential of this topic in various sectors.

Based on a comprehensive analysis of consortium blockchains, TABLE VIIhighlights the advantages, challenges, and implications of three key technologies: PBFT, BLS Signatures, and VRF. Each technology offers unique benefits and faces distinct challenges, shaping their suitability and impact on consortium blockchain environments. PBFT excels in low latency and immediate finality but struggles with scalability in larger networks. BLS Signatures enhance security and reduce communication load but demand high computational power [30], [31], [70]. VRF introduces unpredictability and fairness in leader selection, though its implementation can be complex. These insights provide a nuanced understanding of how these technologies can be leveraged to optimize consortium blockchain performance [11].

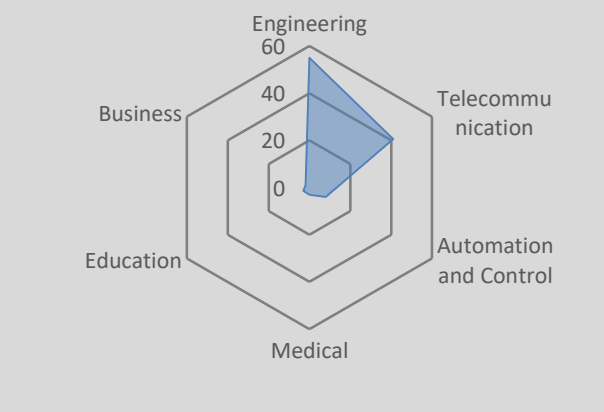


Fig. 9. Research area spreads of the chain studies.

TABLE VII. COMPARISON OF METHOD BASED ON RECORDED ARTICLES

| Technology | Advantages | Challenges | Implications for Consortium Blockchains |
|---|---|---|---|
| **PBFT (Practical Byzantine Fault Tolerance)** | ▪ Low latency and immediate finality<br>▪ Resilient to up to 1/3 faulty nodes.<br>▪ Well-suited for permissioned environments with known participants. | ▪ Scalability issues with large networks due to high communication overhead.<br>▪ Performance degrades as the number of nodes increases. | Ideal for smaller, trust-based consortium environments where high throughput and quick consensus are required. Needs scalability enhancements for larger networks. [12], [32], [52], [53], [63], [70] |
| **BLS (Boneh-Lynn-Shacham) Signatures** | ▪ Enables signature aggregation, reducing the number of transmissions required for consensus.<br>▪ Enhances security and integrity with cryptographic proof. | ▪ Computational overhead for signature verification is high.<br>▪ Requires nodes to manage complex cryptographic operations. | Useful in reducing the communication load in PBFT systems, making them more scalable and efficient. However, demands high computational power and advanced cryptographic understanding. [8], [58] |
| **VRF (Verifiable Random Functions)** | ▪ Provides unpredictability in leader selection, enhancing security.<br>▪ Ensures fairness and reduces risks of manipulation in the consensus process. | ▪ Implementation complexity.<br>▪ May not be universally supported across all blockchain platforms. | Enhances the robustness of the consensus mechanism in PBFT by randomizing the proposer selection, thus preventing targeted attacks and promoting equitable node participation. [9], [10], [71] |

## VI. CONCLUSION

This review has systematically explored the enhancements in scalability of the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm within consortium chains, highlighting pivotal research contributions and their practical implications. Our findings reveal that innovations such as Boneh–Lynn–Shacham (BLS) signatures and Verifiable Random Functions (VRF) significantly improve algorithmic efficiency, thereby enhancing transaction throughput while maintaining the requisite security and reliability in distributed systems. The integration of these technologies marks a substantial contribution to blockchain scalability, offering robust solutions for sectors that demand efficient, large-scale transaction processing such as finance, healthcare, and supply chain management.

While these advancements facilitate the handling of increased workloads without compromising speed or security, challenges persist. The complexity of implementing advanced cryptographic techniques may inhibit wider adoption and potentially introduce new security vulnerabilities that must be thoroughly addressed to prevent exploitation. Future research should therefore focus on optimizing cryptographic protocols within the PBFT framework to enhance both security and operational performance. Exploring hybrid consensus mechanisms that integrate multiple algorithms could provide a balanced approach to scalability and security.

Additionally, investigating the impact of network size on consensus efficiency could yield crucial insights, guiding the design of more adaptive blockchain networks. In conclusion, while the current progress in PBFT scalability is promising, ongoing efforts are necessary to refine these solutions and address emerging challenges. By deepening our understanding and overcoming these limitations, the full potential of PBFT in consortium blockchains can be realized, leading to more robust and scalable blockchain architectures.

## ACKNOWLEDGMENT

This research was supported by the Ministry of Higher Education (MOHE) through Fundamental Research Grant Scheme (FRGS/1/2021/ICT10/UTM/02/3). We also want to thank the Government of Malaysia which provides the MyBrain15 program for sponsoring this work under the self-fund research grant and L0022 from the Ministry of Science, Technology and Innovation (MOSTI). This research was supported by a UTM Fundamental Research Grant Q.J130000.3828.23H38.

## REFERENCES

[1] M. Attaran, “The impact of 5G on the evolution of intelligent automation and industry digitization,” J Ambient Intell Humaniz Comput, vol. 14, no. 5, 2023, doi: 10.1007/s12652-020-02521-x.

[2] D. Song, Y. Wang, and M. Yuan, “An Improved Method of Blockchain Consortium Chain Consensus Mechanism Based on Random Forest Model,” in Communications in Computer and Information Science, 2021. doi: 10.1007/978-981-16-7502-7_17.

[3] Y. Ma, Y. Sun, Y. Lei, N. Qin, and J. Lu, “A survey of blockchain technology on security, privacy, and trust in crowdsourcing services,” World Wide Web, vol. 23, no. 1, 2020, doi: 10.1007/s11280-019-00735-4.

[4] Z. Hussein, M. A. Salama, and S. A. El-Rahman, “Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms,” 2023. doi: 10.1186/s42400-023-00163-y.

[5] F. Q. Ma, Q. L. Li, Y. H. Liu, and Y. X. Chang, “Stochastic performance modeling for practical byzantine fault tolerance consensus in the blockchain,” Peer Peer Netw Appl, vol. 15, no. 6, 2022, doi: 10.1007/s12083-022-01380-x.

[6] P. Chen, Y. Chen, X. Wang, L. Yuan, C. Tan, and Y. Yang, “A high-capacity slicing PBFT protocol based on reputation evaluation model,” Wireless Networks, 2024, doi: 10.1007/s11276-023-03636-7.

[7] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, “A Scalable Multi-Layer PBFT Consensus for Blockchain,” IEEE Transactions on Parallel and Distributed Systems, vol. 32, no. 5, 2021, doi: 10.1109/TPDS.2020.3042392.

[8] M. S. Lacharité, “Security of BLS and BGLS signatures in a multi-user setting,” Cryptography and Communications, vol. 10, no. 1, 2018, doi: 10.1007/s12095-017-0253-6.

[9] P. N. Minh, C. Hiro, and K. Nguyen-An, “Orand - A Fast, Publicly Verifiable, Scalable Decentralized Random Number Generator Based on Distributed Verifiable Random Functions,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2023. doi: 10.1007/978-3-031-46781-3_30.

[10] H. Wang and W. Tan, “Block proposer election method based on verifiable random function in consensus mechanism,” in Proceedings of 2020 IEEE International Conference on Progress in Informatics and Computing, PIC 2020, 2020. doi: 10.1109/PIC50277.2020.9350766.

[11] C. Jiang, C. Guo, C. Shan, and Y. Zhang, “VPBFT: Improved PBFT Consensus Algorithm Based on VRF and PageRank Algorithm,” in Communications in Computer and Information Science, 2024. doi: 10.1007/978-981-99-8104-5_18.

[12] L. Yang and H. Huang, “Adapted PBFT Consensus Protocol for Sharded Blockchain,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2022. doi: 10.1007/978-3-031-17551-0_3.

[13] R. Garratt, “Fabian Schär and Aleksander Berentsen: Bitcoin, Blockchain, and Cryptoassets: A Comprehensive Introduction,” Business Economics, vol. 57, no. 1, 2022, doi: 10.1057/s11369-021-00236-1.

[14] A. Olbrecht and G. Pieters, “Crypto-Currencies and Crypto-Assets: An Introduction,” 2023. doi: 10.1057/s41302-023-00246-1.

[15] S. Zhang and J. H. Lee, “Mitigations on Sybil-Based Double-Spend Attacks in Bitcoin,” IEEE Consumer Electronics Magazine, vol. 10, no. 5, 2021, doi: 10.1109/MCE.2020.2988031.

[16] D. Bazzanella and A. Gangemi, “Bitcoin: a new proof-of-work system with reduced variance,” Financial Innovation, vol. 9, no. 1, 2023, doi: 10.1186/s40854-023-00505-2.

[17] S. Mssassi and A. A. El Kalam, “Leveraging Blockchain for Enhanced Traceability and Transparency in Sustainable Development,” 2024. doi: 10.1007/978-3-031-54318-0_14.

[18] R. Pathak, B. Soni, and N. B. Muppalaneni, “Significance and Challenges in Blockchain-Based Secure Sharing of Healthcare Data,” in Lecture Notes in Electrical Engineering, 2024. doi: 10.1007/978-981-99-7137-4_74.

[19] P. M. Chanal and M. S. Kakkasageri, “Blockchain-based data integrity framework for Internet of Things,” Int J Inf Secur, vol. 23, no. 1, 2024, doi: 10.1007/s10207-023-00719-6.

[20] S. Tucci-Piergiovanni, “Keynote: Blockchain consensus protocols, from Bitcoin to Ethereum 2.0,” 2022. doi: 10.1109/percomworkshops53856.2022.9775195.

[21] D. Kamboj, M. Chauhan, and K. K. Gola, “Ethereum’s Blockchain Network Mechanism for High-Performance Authentication and Efficient Block Creation,” SN Comput Sci, vol. 4, no. 5, 2023, doi: 10.1007/s42979-023-01889-9.

[22] Z. A. Khan and A. Siami Namin, “Ethereum smart contracts: Vulnerabilities and their classifications,” in Proceedings - 2020 IEEE International Conference on Big Data, Big Data 2020, 2020. doi: 10.1109/BigData50022.2020.9439088.

[23] N. P. Sheppard, "Can Smart Contracts Learn from Digital Rights Management?," IEEE Technology and Society Magazine, vol. 39, no. 1, 2020, doi: 10.1109/MTS.2020.2967515.

[24] N. Nousias, G. Tsakalidis, S. Petridou, and K. Vergidis, "Modelling the Development and Deployment of Decentralized Applications in Ethereum Blockchain: A BPMN-Based Approach," in Lecture Notes in Business Information Processing, 2022. doi: 10.1007/978-3-031-06530-9_5.

[25] T. Min and W. Cai, "Portrait of decentralized application users: an overview based on large-scale Ethereum data," CCF Transactions on Pervasive Computing and Interaction, vol. 4, no. 2, 2022, doi: 10.1007/s42486-022-00094-6.

[26] E. Kafeza, S. J. Ali, I. Kafeza, and H. Alkatheeri, "Legal smart contracts in ethereum block chain: Linking the dots," in Proceedings - 2020 IEEE 36th International Conference on Data Engineering Workshops, ICDEW 2020, 2020. doi: 10.1109/ICDEW49219.2020.00-12.

[27] B. C. Ghosh, T. Bhartia, S. K. Addya, and S. Chakraborty, "Leveraging public-private blockchain interoperability for closed consortium interfacing," in Proceedings - IEEE INFOCOM, 2021. doi: 10.1109/INFOCOM42981.2021.9488683.

[28] M. T. Ta and T. Q. Do, "A study on gas cost of ethereum smart contracts and performance of blockchain on simulation tool," Peer Peer Netw Appl, vol. 17, no. 1, 2024, doi: 10.1007/s12083-023-01598-3.

[29] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," Peer Peer Netw Appl, vol. 14, no. 5, 2021, doi: 10.1007/s12083-021-01127-0.

[30] Z. F. Wang, S. Q. Liu, P. Wang, and L. Y. Zhang, "BW-PBFT: Practical byzantine fault tolerance consensus algorithm based on credit bidirectionally waning," Peer Peer Netw Appl, vol. 16, no. 6, 2023, doi: 10.1007/s12083-023-01566-x.

[31] J. Liu, X. Deng, W. Li, and K. Li, "CG-PBFT: an efficient PBFT algorithm based on credit grouping," Journal of Cloud Computing, vol. 13, no. 1, 2024, doi: 10.1186/s13677-024-00643-7.

[32] G. Zhang, S. Ji, H. Dong, and P. Zhang, "An Improved PBFT Consensus Algorithm for Supply Chain Finance," in Communications in Computer and Information Science, 2024. doi: 10.1007/978-981-99-8104-5_25.

[33] S. Wadhwa and Gagandeep, "Empirical Analysis on Consensus Algorithms of Blockchain," in Lecture Notes in Networks and Systems, 2022. doi: 10.1007/978-981-16-4284-5_44.

[34] H. Guo and X. Yu, "A survey on blockchain technology and its security," Blockchain: Research and Applications, vol. 3, no. 2, 2022, doi: 10.1016/j.bcra.2022.100067.

[35] H. Zhai and X. Tong, "A Practical Byzantine Fault Tolerant Algorithm Based on Credit Value and Dynamic Grouping," in Communications in Computer and Information Science, 2024. doi: 10.1007/978-981-97-0885-7_23.

[36] M. Abbasi, J. Prieto, M. Plaza-Hernández, and J. M. Corchado, "A Novel Aging-Based Proof of Stake Consensus Mechanism," in Lecture Notes in Networks and Systems, 2023. doi: 10.1007/978-3-031-36957-5_5.

[37] L. Lei, C. Lan, and L. Lin, "Chained Tendermint: A Parallel BFT Consensus Mechanism," in 2020 3rd International Conference on Hot Information-Centric Networking, HotICN 2020, 2020. doi: 10.1109/HotICN50779.2020.9350801.

[38] P. Boos and M. Lacoste, "Networks of Trusted Execution Environments for Data Protection in Cooperative Vehicular Systems," in Advances in Intelligent Systems and Computing, 2020. doi: 10.1007/978-981-15-3750-9_8.

[39] W. Liang et al., "PDPChain: A Consortium Blockchain-Based Privacy Protection Scheme for Personal Data," IEEE Trans Reliab, vol. 72, no. 2, 2023, doi: 10.1109/TR.2022.3190932.

[40] R. Qiao, X. Y. Luo, S. F. Zhu, A. Di Liu, X. Q. Yan, and Q. X. Wang, "Dynamic autonomous cross consortium chain mechanism in e-healthcare," IEEE J Biomed Health Inform, vol. 24, no. 8, 2020, doi: 10.1109/JBHI.2019.2963437.

[41] Y. Li, L. Qiao, and Z. Lv, "An Optimized Byzantine Fault Tolerance Algorithm for Consortium Blockchain," Peer Peer Netw Appl, vol. 14, no. 5, 2021, doi: 10.1007/s12083-021-01103-8.

[42] G. Sun, M. Dai, J. Sun, and H. Yu, "Voting-Based Decentralized Consensus Design for Improving the Efficiency and Security of Consortium Blockchain," IEEE Internet Things J, vol. 8, no. 8, 2021, doi: 10.1109/JIOT.2020.3029781.

[43] K. Wang et al., "A trusted consensus fusion scheme for decentralized collaborated learning in massive IoT domain," Information Fusion, vol. 72, 2021, doi: 10.1016/j.inffus.2021.02.011.

[44] A. Binun, S. Dolev, and T. Hadad, "Self-stabilizing byzantine consensus for blockchain," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019. doi: 10.1007/978-3-030-20951-3_10.

[45] R. Wang, W. T. Tsai, F. Zhang, L. Yu, H. Zhang, and Y. Zhang, "Adaptive Byzantine Fault-Tolerant ConsensusProtocol," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2023. doi: 10.1007/978-3-031-28124-2_7.

[46] C. Lin, D. He, X. Huang, X. Xie, and K.-K. R. Choo, "PPChain: A Privacy-Preserving Permissioned Blockchain Architecture for Cryptocurrency and Other Regulated Applications," IEEE Syst J, vol. 15, no. 3, 2020, doi: 10.1109/jsyst.2020.3019923.

[47] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan, "A Proof-of-Quality-Factor (PoQF)-Based Blockchain and Edge Computing for Vehicular Message Dissemination," IEEE Internet Things J, vol. 8, no. 4, 2021, doi: 10.1109/JIOT.2020.3026731.

[48] P. Zhu, J. Hu, Y. Zhang, and X. Li, "A blockchain based solution for medication anti-counterfeiting and traceability," IEEE Access, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3029196.

[49] W. Chen, Z. Yang, J. Zhang, J. Liang, Q. Sun, and F. Zhou, "Enhancing Blockchain Performance via On-chain and Off-chain Collaboration," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2023. doi: 10.1007/978-3-031-48421-6_27.

[50] L. Jia, K. Wang, X. Wang, L. Yu, Z. Li, and Y. Sun, "Themis: An Equal, Unpredictable, and Scalable Consensus for Consortium Blockchain," in Proceedings - International Conference on Distributed Computing Systems, 2022. doi: 10.1109/ICDCS54860.2022.00031.

[51] Y. Li et al., "Research on Performance Scalability of State Grid chain-Data Side chain," in Proceedings - 2020 International Conference on Computer Science and Management Technology, ICCSMT 2020, 2020. doi: 10.1109/ICCSMT51754.2020.00054.

[52] Q. Zhang, J. Su, Z. Ma, Y. Zhang, J. Yang, and J. Zhan, "Blockchain Model Testing and Implementation Based on Improved PBFT Consensus," in Proceedings of the 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, 2021. doi: 10.1109/IDAACS53288.2021.9660959.

[53] G. Yu, B. Wu, and 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. doi: 10.1109/CTISC49998.2020.00009.

[54] S. A. Krishnan Thyagarajan and G. Malavolta, "Lockable signatures for blockchains: Scriptless scripts for all signatures," in Proceedings - IEEE Symposium on Security and Privacy, 2021. doi: 10.1109/SP40001.2021.00065.

[55] F. Armknecht, J. M. Bohli, G. Karame, and W. Li, "Outsourcing Proofs of Retrievability," IEEE Transactions on Cloud Computing, vol. 9, no. 1, 2021, doi: 10.1109/TCC.2018.2865554.

[56] M. S. Yoosuf and R. Anitha, "LDuAP: lightweight dual auditing protocol to verify data integrity in cloud storage servers," J Ambient Intell Humaniz Comput, vol. 13, no. 8, 2022, doi: 10.1007/s12652-021-03321-7.

[57] K. Deng, M. Xu, and S. Fu, "Outsourced Data Integrity Auditing for Efficient Batch Dynamic Updates," in Communications in Computer and Information Science, 2020. doi: 10.1007/978-981-15-3418-8_21.

[58] P. Wang, X. Su, M. Jourenko, Z. Jiang, M. Larangeira, and K. Tanaka, "Environmental Adaptive Privacy Preserving Contact Tracing System: A Construction From Public Key Rerandomizable BLS Signatures," IEEE Access, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3164186.

[59] F. Guo and W. Susilo, "Optimal Tightness for Chain-Based Unique Signatures," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2022. doi: 10.1007/978-3-031-07085-3_19.

[60] C. B. Avoussoukpo, C. Xu, M. Tchenagnon, and N. Eltayieb, "Towards an Aggregate Signature-based Authentication for Opportunistic Networks," in 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020, 2020. doi: 10.1109/CyberSA49311.2020.9139650.

[61] S. A. Abdel Hakeem and H. Kim, "Authentication and encryption protocol with revocation and reputation management for enhancing 5G-V2X security," Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 7, 2023, doi: 10.1016/j.jksuci.2023.101638.

[62] L. Krzywiecki and H. Salin, "Short Signatures via Multiple Hardware Security Modules with Key Splitting in Circuit Breaking Environments," in Proceedings - 2022 IEEE 21st International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2022, 2022. doi: 10.1109/TrustCom56396.2022.00218.

[63] W. Ziyang, W. Juan, L. Yaning, and W. Wei, "Improvement of PBFT Consensus Mechanism Based on Credibility," in 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing, ICCWAMTIP 2021, 2021. doi: 10.1109/ICCWAMTIP53232.2021.9674168.

[64] H. Bansal, D. Gupta, and D. Anand, "Analysis of Consensus Algorithms in context of the Blockchain based Applications," in 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), ICRITO 2022, 2022. doi: 10.1109/ICRITO56286.2022.9964653.

[65] N. Zhao, H. Wu, L. Wang, and X. Sun, "A robust incentive consensus propagation design for consortium-chain based wireless network," in 2020 IEEE International Conference on Communications Workshops, ICC Workshops 2020 - Proceedings, 2020. doi: 10.1109/ICCWorkshops49005.2020.9145392.

[66] C. Xu, Y. Qu, T. H. Luan, P. W. Eklund, Y. Xiang, and L. Gao, "A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things," IEEE Internet Things J, vol. 9, no. 6, 2022, doi: 10.1109/JIOT.2021.3103275.

[67] J. K. Lee, N. Kim, S. Cho, and J. W. Kang, "Deep video prediction network-ased inter-frame coding in HEVC," IEEE Access, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2993566.

[68] L. Chen, Q. Fu, Y. Mu, L. Zeng, F. Rezaeibagha, and M. S. Hwang, "Blockchain-based random auditor committee for integrity verification," Future Generation Computer Systems, vol. 131, 2022, doi: 10.1016/j.future.2022.01.019.

[69] U. Balande and D. shrimankar, "A modified teaching learning metaheuristic algorithm with opposite-based learning for permutation flow-shop scheduling problem," Evol Intell, vol. 15, no. 1, 2022, doi: 10.1007/s12065-020-00487-5.

[70] V. Rao, A. R. Shenoy, and M. Kiran, "Efficient PBFT: A Novel and Efficient Approach to the PBFT Consensus Algorithm," in Smart Innovation, Systems and Technologies, 2022. doi: 10.1007/978-981-16-4177-0_77.

[71] H. Narumanchi, L. P. Maddali, and N. Emmadi, "Private and Verifiable Inter-bank Transactions and Settlements on Blockchain," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2023. doi: 10.1007/978-3-031-49099-6_29.