Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2024.054556

REVIEW

A Systematic Literature Review on Blockchain Consensus Mechanisms' Security: Applications and Open Challenges

Muhammad Muntasir Yakubu[1,2,*], Mohd Fadzil B Hassan[1,3], Kamaluddeen Usman Danyaro[1], Aisha Zahid Junejo[4], Muhammed Siraj[5], Saidu Yahaya[1], Shamsuddeen Adamu[1] and Kamal Abdulsalam[6]

[1]Department of Computer and Information Science, Universiti Teknologi PETRONAS, Perak, 32610, Malaysia

[2]Department of Information Technology, Faculty of Computing, Federal University Dutsin-Ma, Katsina, 5001, Nigeria

[3]Institute of Autonomous Systems, Universiti Teknologi PETRONAS, Perak, 32610, Malaysia

[4]Institut für Luftfahrtsysteme, Universität Stuttgart, Stuttgart, 70569, Germany

[5]Department of Computer Science, Academic City University College, Agbogba, Accra, 421, Ghana

[6]Department of Mathematical Sciences, National University of the Center of the Province of Buenos Aires, Pinto, Tandil, 399, Argentina

*Corresponding Author: Muhammad Muntasir Yakubu. Email: muhammad_22010099@utp.edu.my

Received: 31 May 2024 Accepted: 25 July 2024 Published: 22 November 2024

ABSTRACT

This study conducts a systematic literature review (SLR) of blockchain consensus mechanisms, an essential protocols that maintain the integrity, reliability, and decentralization of distributed ledger networks. The aim is to comprehensively investigate prominent mechanisms' security features and vulnerabilities, emphasizing their security considerations, applications, challenges, and future directions. The existing literature offers valuable insights into various consensus mechanisms' strengths, limitations, and security vulnerabilities and their real-world applications. However, there remains a gap in synthesizing and analyzing this knowledge systematically. Addressing this gap would facilitate a structured approach to understanding consensus mechanisms' security and vulnerabilities comprehensively. The study adheres to Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines and computer science standards and reviewed 3749 research papers from 2016 to 2024, excluding grey literature, resulting in 290 articles for descriptive analysis. The research highlights an increased focus on blockchain consensus security, energy efficiency, and hybrid mechanisms within 60% of research papers post-2019, identifying gaps in scalability, privacy, and interoperability for future exploration. By synthesizing the existing research and identifying the key trends, this SLR contributes to advancing the understanding of blockchain consensus mechanisms' security and guiding future research and structured innovation in blockchain systems and applications.

KEYWORDS

Blockchain consensus mechanisms; supply chain management; proof of work (PoW); proof of stake (PoS); practical byzantine fault tolerance (PBFT)

1 Introduction

Blockchain consensus mechanisms trace back to the inception of Bitcoin, the first-ever cryptocurrency, introduced by an unknown person or group using the pseudonym Nakamoto in 2008 [1]. Bitcoin's groundbreaking innovation was its implementation of a decentralized digital ledger, such as the blockchain, which enabled peer-to-peer (P2P) transactions without intermediaries like financial institutions or banks [2]. Since then, the evolution of blockchain consensus mechanisms reflects ongoing efforts to address the security, scalability, and sustainability challenges inherent in the decentralized digital ledger networks. As the blockchain ecosystem evolves, consensus mechanisms will remain a critical area of innovation and research, shaping the future of decentralized systems and applications [3]. Consensus mechanisms are the cornerstone of blockchain networks, ensuring their integrity, reliability, and decentralization [4]. Blockchain consensus mechanisms are protocols distributed networks use to validate transactions and ensure trust [5]. Examples of these mechanisms include Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Space-Time (PoST), Proof of Authority (PoA), etc. Each mechanism has security, decentralization, and scalability trade-offs, chosen based on network requirements. These mechanisms play a crucial role in blockchain technology by enabling network participants to agree on the validity of transactions and the current distributed ledger [6]. These mechanisms are fundamental to the functioning of blockchain networks, determining how new transactions are secured, validated, added to the blockchain, and maintained over time. One of the primary functions of consensus mechanisms is to guarantee the security of blockchain networks [7]. By establishing a mechanism through which agreement is reached on the validity of transactions, consensus protocols help prevent malicious actors from tampering with the blockchain's transaction history or double-spending digital assets [7,8]. Through cryptographic principles and distributed consensus algorithms, blockchain consensus mechanisms provide a robust defense against various security threats, including Sybil attacks, double-spending attacks, and 51% attacks [9].

However, despite the critical role of consensus mechanisms in ensuring blockchain security, the landscape of blockchain technology is constantly evolving, with new consensus algorithms and security challenges emerging regularly. Extensively, the sets of consensus mechanisms are set to be over 130 algorithms, which are discerned and classified [3]. Moreover, this number is still growing. As such, there is a pressing need for a systematic review of existing research in blockchain consensus mechanisms security. Considering how quickly things are developing in the blockchain area, it is critical to thoroughly understand state-of-the-art research on consensus mechanisms security. As Blockchain technology ensures decentralized transactions with a consensus mechanism, establishing rules for nodes to agree on transaction validity and maintain a tamper-resistant ledger [10]. The existing literature offers valuable insights into the strengths, limitations, and security vulnerabilities of various consensus mechanisms such as PoW, PoS, PBFT, and DPoS, as well as their real-world applications [11–13]. However, there remains to be a gap in systematically synthesizing and analyzing this knowledge. Addressing this gap would facilitate a structured approach to understanding consensus mechanisms.

A systematic literature review would offer a structured approach to synthesizing and analyzing existing knowledge, enabling researchers to identify trends, gaps, and areas for further investigation. By systematically examining the literature, researchers can gain insights into the strengths and limitations of different consensus mechanisms, the security vulnerabilities they may exhibit, and the real-world applications in which they are employed. The study reviewed 3749 research papers from January 2016 to February 2024, excluding grey literature. After a comprehensive screening and cleaning process, 290 articles were studied for descriptive analysis. It offers insights into current trends, interdisciplinary aspects, and thematic distributions in blockchain consensus mechanism security research. This paper contributes comprehensively by analyzing blockchain consensus mechanisms, addressing security, applications, challenges, and future directions, and guiding future research and innovation, as shown in Table 1, showing the unique contribution of the current study. The research questions guiding this study include:

i) What specific security vulnerabilities are associated with blockchain consensus mechanisms?
ii) How do security considerations influence the selection and implementation of specific consensus mechanisms in different real-world applications such as supply chains or healthcare?
iii) What are the open issues and challenges in the security of blockchain consensus mechanisms?

This study intends to answer these research questions to offer essential insights into the security features of blockchain consensus mechanisms and their consequences for practical applications in various fields. Employing a systematic review methodology, we shed light on the existing literature to advance the ongoing blockchain security and governance discourse. It is important to note that while this review provides valuable insights into consensus security and vulnerabilities, it may not comprehensively cover all developments in the rapidly evolving field of blockchain security. In the research paper, our study provides a comprehensive and in-depth analysis of the security considerations, applications, challenges, and future directions of blockchain consensus mechanisms, focusing specifically on their security aspects. Unlike previous reviews, our paper offers a systematic literature review following Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, providing a structured approach to synthesizing existing knowledge and guiding future research and innovation in decentralized systems and applications [14,15] (Supplementary Materials). So, the research addresses the security vulnerabilities of blockchain consensus mechanisms, focusing on identifying, analyzing, and providing solutions to these issues within the context of real-world applications.

Table 1: Comparative analyses of previous reviews on consensus mechanisms

Citation	Focus	Method	Contribution	Year	Research paper
[16]	Technical comparison of consensus mechanisms in literature	Comparative analysis	Identifies and discusses performance and security parameters and analyses and compares common consensus mechanisms. It also highlights research gaps and serves as a guide for developers and researchers.	2018	–

(Continued)

Table 1 (continued)

Citation	Focus	Method	Contribution	Year	Research paper
[11]	Comprehensive survey and comparison of consensus mechanisms in blockchain	Survey and comparison	Evaluate features, performance, and security factors of popular consensus algorithms and provide classification, detailed discussion, and recommendations for development.	2019	–
[17]	Explores consensus mechanisms and security protocols in Distributed Ledger Technology (DLT)	Review	It surveys consensus mechanisms and security protocol applications across various blockchain contexts, including cryptocurrencies, consortiums, and private blockchains.	2019	–
[5]	Aiming to enhance understanding and facilitate the design of future protocols	Comprehensive review and analysis	It provides a detailed analysis of blockchain consensus protocols, highlighting differences, application scenarios, security, fault tolerance, scalability, and trade-offs. It aims to guide developers in designing future protocols.	2020	–
[8]	Evaluation of blockchain consensus algorithms' frameworks	Survey and evaluation	The paper proposes a unified consensus algorithm process model for blockchain, analyses mainstream algorithms, and discusses security design principles for diverse application scenarios.	2021	–

(Continued)

Table 1 (continued)

Citation	Focus	Method	Contribution	Year	Research paper
[3]	Comprehensive review and classification of blockchain consensus mechanisms	Review and analysis	Comparing blockchain to traditional distributed ledgers, classifying consensus algorithms comprehensively, and providing an architectural framework for evaluating existing and future consensus mechanisms.	2021	–
[12]	Review and analysis of consensus mechanisms in blockchain systems	Short review	Examination of the three categories of consensus algorithms, focusing on their principles, characteristics, performance metrics, limitations, and suitability for different blockchain applications. Guides algorithm selection and outlines future research areas.	2022	–
[18]	Overview and analysis of blockchain consensus mechanisms	Review and analysis	Discuss consensus process principles, classify mainstream algorithms, review research progress, compare characteristics and suitability, and identify future trends.	2022	–
[12]	In-depth analysis of existing blockchain consensus algorithm	Review and analysis	It provides insights into various consensus algorithms, offers a taxonomy, and explores healthcare, IoT, and data management applications. It aims to aid researchers and developers in selecting suitable algorithms.	2022	–

(Continued)

Table 1 (continued)

Citation	Focus	Method	Contribution	Year	Research paper
[18]	Ensuring node consensus in complex networks	Review	The paper summarises blockchain fundamentals and underscores the significance of consensus algorithms. It provides insights into recent developments in consensus algorithm research to inform future advancements.	2022	–
[6]	Blockchain consensus mechanisms explored	Comparative study	Comparison of consensus mechanisms, their impact on security and performance, and exploring potential societal, organizational, and industrial applications.	2023	–
[19]	Explore blockchain and consensus development	Systematic review	It provides insights into blockchain development, particularly for businesses, by comparing consensus mechanisms and aiding their selection.	2023	–
[2]	Delves into blockchain's evolution, consensus mechanisms, and real-world applications	Review and analysis	Reviews deployable algorithms on open-source platforms, aiding researchers in selecting architectures and consensus mechanisms. It also highlights blockchain's benefits across various sectors like finance, supply chain management, and healthcare.	2023	–

(Continued)

Table 1 (continued)

Citation	Focus	Method	Contribution	Year	Research paper
[20]	Review and comparison of consensus mechanisms for blockchain	Comparative analysis	The study evaluates various algorithms based on goals, power consumption, cost, application scenarios, and research directions, offering an overview of the current state, future challenges, and algorithm selection recommendations.	2024	–
[20]	Examining blockchain consensus algorithm selection	Comparative analysis	Insights into the state and upcoming difficulties of blockchain technology consensus algorithms and recommendations for choosing the best algorithm for various blockchain applications.	2024	–
Present study	Blockchain consensus mechanisms' security: applications and open challenges	Systematic literature review (SLR)	A comprehensive analysis of blockchain consensus mechanisms' security considerations, applications, challenges, and future directions through a systematic literature review following PRISMA guidelines provides insights. It guides future research and innovation in decentralized systems and applications.	2024	This paper conducts an SLR focusing specifically on the security considerations of blockchain consensus mechanisms, offering insights and guidance for future research and innovation.

This paper offers a comprehensive systematic literature review (SLR) of blockchain consensus mechanisms, focusing on their security considerations. It identifies and analyzes security vulnerabilities in key mechanisms such as PoW, PoS, DPoS, and PBFT and highlights research gaps in scalability, privacy, interoperability, energy efficiency, and formal verification. The study provides practical insights for selecting appropriate consensus mechanisms by evaluating real-world applications like supply chains, healthcare, etc. Following PRISMA guidelines, the study enhances the credibility of its findings and suggests future research directions, including hybrid approaches and decentralized governance models. This research significantly contributes to the literature by synthesizing existing knowledge, identifying critical gaps, and guiding future innovation in blockchain technology.

The remainder of this work is organized as follows. Section 2 briefly overviews blockchain consensus mechanisms and explores their security properties with vulnerabilities. Section 3 describes the methodology used to carry out the systematic literature review. The findings from the descriptive analysis are in Section 4. Then, the consensus mechanisms for security are listed in Section 5. The security considerations and evaluation of each consensus mechanism's security features are presented in Section 6, while in Section 7, applications and use cases are presented. Relevant open issues, trends, and further research lines are discussed in Section 8, and research is concluded in Section 9.

2 Overview of Blockchain Consensus Mechanisms

Each new block creates a secure and unchangeable chain of records in the blockchain world. A block is a distributed append-only timestamped data structure containing a previous block's cryptographic hash [21]. Consensus mechanisms are critical protocols that allow all participants in decentralized blockchain networks to agree on the current state of the shared ledger. They establish trust and reach a consensus among the nodes on the validity of new blocks added to the chain [3]. Without consensus, a blockchain would be chaotic, prone to double-spending, and vulnerable to attacks [2,6]. These mechanisms are essential to the operation of blockchain networks. As shown in Fig. 1, it fits into the distributed systems architecture; the consensus layer provides security by preventing malicious activities [7,10,22]. In consortium blockchains, various consensus algorithms have been developed, each with strengths and weaknesses [23]. In the basic consensus mechanisms, the consistency agreement has been evaluated based on security, scalability, and performance [22]. Despite the potential of blockchain technology, challenges such as security and scalability remain in this ecosystem [24].

In a blockchain network with no central authority, the nodes need a way to collectively validate and agree on the sequence of transactions and blocks. This prevents scenarios where different nodes have diverging views of the blockchain state, which could enable double-spending of digital assets [9]. Consensus mechanisms provide the rules for securely updating the shared ledger in a decentralized manner. It prevents malicious actors from manipulating the ledger. By agreeing on a single version of truth, the network becomes resistant to attacks. Blockchain operates in a decentralized approach, meaning there is no central authority. Participants across the network validate and record transactions. Consensus ensures that these nodes agree on the order and content of operations. Trust is minimized in blockchain systems. Participants do not need to trust each other explicitly; they rely on the consensus rules to validate transactions. This trustlessness is essential for security and transparency [3,7,10]. Research [25] highlights the need for these consensus protocols in permissionless blockchains, with PoS being a promising alternative to the energy-intensive PoW, another research [26] discusses the theoretical underpinnings of blockchain consensus, emphasizing the importance of understanding the guarantees offered by different consensus algorithms. The research of [3] provides a comprehensive review of 130 consensus algorithms, underscoring their role in the stable operation of blockchain systems. This further explores the evolution of consensus mechanisms from PoW to Blockchain 3.0 and their impact on the stability and consistency of blockchain systems [27].

The need for consensus mechanisms in blockchains arises from the famous Byzantine General's Problem in distributed computing. It states that in a distributed network with malicious nodes that can propagate false information, the non-malicious nodes need a reliable mechanism to reach consensus, even when some nodes are malicious or faulty "Byzantines." The challenge is to get a consensus despite the presence of malicious actors. In the context of blockchain, nodes represent the generals, and achieving consensus is similar to coordinating their actions despite potential traitors [26]. Consensus mechanisms can be categorized based on their underlying principles. Some research [7,22] identifies PoW, PoS, Byzantine, etc., consistency agreement as the basic consensus mechanisms, evaluating them on various aspects. In PoW, miners compete to solve challenging mathematical puzzles, as Table 1 illustrates. Blocks are added to the chain by miners in order of validity. The quantity of coins held by validators, or stakers, determines their selection in Proof of Stake (PoS). They verify transactions and add new blocks. Here, holders of DPoS tokens cast votes for delegates with transaction validation authority. Nodes of PBFT interact and cast votes on proposed blocks. The agreement of a super-majority constitutes consensus. Nodes choose a leader in Raft, which is the leader-based consensus, and the leader suggests blocks. Validators in Proof of Authority (PoA) are recognized entities, such as authorized organizations, who create blocks in shifts. Some private and consortium blockchains make use of these. Further Reference [28] reviews these mechanisms, highlighting their strengths, limitations, and performance measures. Reference [29] proposes a cluster-based classification of consensus algorithms, identifying new clusters, and discussing open problems. Research [30] explores the potential for mechanism design approaches to achieving consensus, particularly in mitigating trade-offs and enhancing scalability. Every consensus method involves trade-offs; the decision is based on the particular use case, the objectives of the network, and the desired characteristics. As blockchain technology develops further, additional consensus techniques can appear.

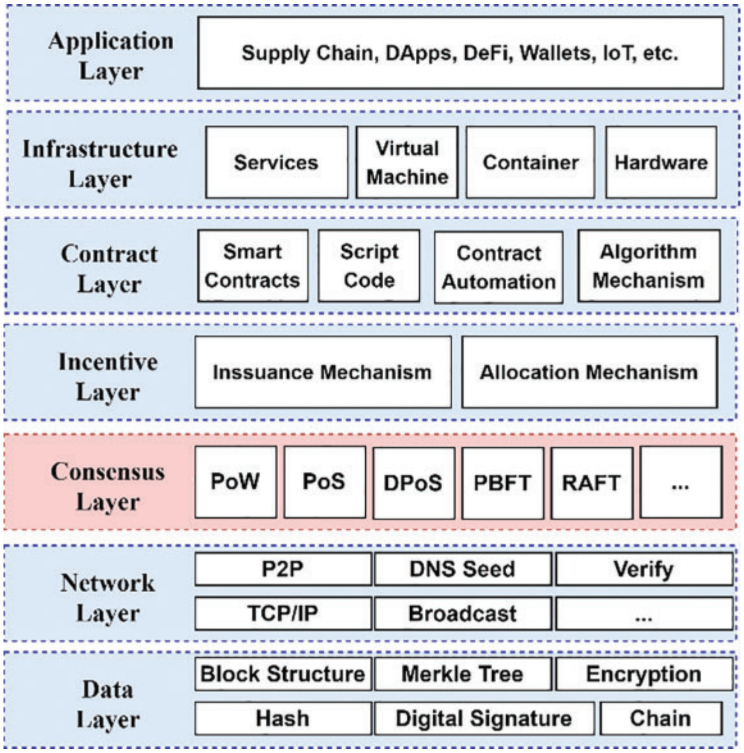

Figure 1: How consensus fits into distributed systems

Based on the existing literature [3,8,23,28], Table 2 classifies consensus mechanisms based on their underlying principles, outlining examples and pros and cons for each mechanism. It concisely overviews popular mechanisms such as PoW, PoS, DPoS, PBFT, Raft, and PoA, highlighting their essential characteristics and trade-offs. This classification aids in understanding the diverse approaches to achieving consensus in blockchain networks.

Table 2: Classification of consensus mechanisms based on their underlying principles

Consensus mechanism	Principle	Example	Pros	Cons
PoW	Miners solve puzzles and add blocks if the first to succeed.	Bitcoin uses PoW	Security, decentralization	High energy consumption, scalability challenges
PoS	Validators selected by coin holdings create blocks and validate transactions.	The impending upgrade of Ethereum to Ethereum 2.0	Energy-efficient, scalability potential	Initial wealth concentration
DPoS	Token holders elect delegates to validate transactions.	Enterprise Operating System (EOS), Transparent Representative Offer Network (TRON)	Fast, scalable	Centralization risk
PBFT	Nodes communicate and vote on proposed blocks. Consensus is reached when a supermajority agrees.	Hyperledger fabric	Fast, suitable for private blockchains	Requires a fixed set of validators
Raft	Leader-based consensus. Nodes elect a leader, and the leader proposes blocks.	Used in some permissioned blockchains	Simplicity, fault tolerance	Limited scalability
PoA	Validators are known individuals (e.g., approved organizations). They choose turns to create blocks.	Used in some private and consortium blockchains	Fast, low energy consumption	Centralization

3 Research Methodology

This section outlines the procedure for selecting articles for a systematic literature review. Papers were chosen iteratively, and parts of the review were presented transparently. We aim to scientifically review blockchain-based consensus mechanism security, following the Preferred Reporting Items for Systematic Review and Meta-Analyses (PRISMA) guidelines. This review aligns with computer science standards using guidelines from Kitchenham and Charters [31]. The overall methodological approach includes the following steps:

- Recognize the necessity for the review, draft a proposal, and formulate the review protocol.
- Locate relevant research, choose studies, evaluate their quality, take notes, extract data, and synthesize findings.
- Present the review's outcomes and deductions.

3.1 Information Source

Papers were extracted from various reputable databases, including articles and conference proceedings. Choosing highly indexed, reputable databases ensures the quality and relevance of this research. However, the review efforts are restricted to the following highly indexed databases:

- Scopus
- ISI Web of Science
- Google Scholar
- ACM Digital Library
- IEEE Explore Digital Library
- Science Direct

3.2 Search Strategy

Primary studies were collected by conducting keyword searches in databases, yielding a diverse range of results due to the use of broad search terms. The leading search word was inserted between the "AND" and "OR" operators. The search terms were selected based on the scope of the research and intervention, including terms related to: ("Blockchain", OR "Block chain" OR "Block-chain" OR "Blockchain security", OR "Secur∗" "Security threat" OR "Security attack") AND ("Consensus Mechanism∗" OR "Consensus Algorithm∗" OR "Consensus Protocol∗"). The search was conducted between 04 November 2023, and 19 January 2024, with publications from 2016 onwards included. Filtering was employed to refine the results, applying inclusion and exclusion criteria detailed in the subsequent section. Used broad, comprehensive search terms to capture various relevant studies.

3.3 Study Eligibility Criteria

Consensus mechanisms are utilized in distributed ledgers, like blockchain, to enhance privacy and security. This study aims to summarize and evaluate these applications. Eligible studies addressed blockchain-based consensus mechanisms for security vulnerabilities, explicitly examining types of vulnerabilities in PoW, PoS, DPoS, etc. Additional criteria restricted eligible studies to peer-reviewed publications, conference proceedings, book chapters, reports, theses, and dissertations in English, published between 2016 and 2024. Conference abstracts, commentaries, archived proposals, books, short surveys, letters, retracted notes, errata, and editorials were excluded. The review focused solely on Computer Science and excluded articles addressing security or privacy for consensus mechanisms in distributed ledgers other than blockchain technology, aiming to highlight the benefits of blockchain consensus mechanisms. The research focused on peer-reviewed, English-language publications to ensure credibility and accessibility.

3.4 Selection Results

The study selection process involved three stages: screening titles and keywords, screening abstracts, and full-text reading. Initially, all retrieved studies were screened based on their titles and keywords. Following this, a comprehensive review of the identified studies was conducted. Initially, 3749 studies were identified (Scopus 651, ISI Web of Science 873; Google Scholar 456; ACM Digital Library 584; IEEE Explorer Digital Library 782; and Science Direct 403). After applying inclusion and exclusion criteria to the titles and keywords, the research pool was reduced to 594 articles, with 3345 exclusions. Considering duplicate articles further reduced the number to 441, excluding 153 duplicates. Evaluating abstracts using inclusion/exclusion criteria led to the exclusion of 108 articles, resulting in 333 articles for full-text review, as shown in Table 3 below. Of these, 68 articles were excluded, leaving 265 primary studies for the systematic literature review (SLR). An additional 25 eligible articles were identified from other sources, resulting in a total of 290 articles. Several studies were excluded for focusing primarily on technical aspects of distributed systems, blockchain technology, and subtopics like smart contract security, IoT, and cybersecurity. The research employed a multi-stage screening process to systematically narrow the pool to the most relevant studies. The search strategy flowchart is shown in Fig. 2.

Table 3: Inclusion and exclusion criteria

Selection criteria	Scientific database	Additional literature
Inclusion	1. Document Type: Peer-reviewed research articles (including articles in press), book chapters, conference proceedings papers, review papers, etc. 2. Year Range: 2016 – 2024 (time-frame restrictions) 3. Subject Area: Computer Science 4. Publication Stage: Final	English reports without time-frame restrictions
Exclusion	1. During title screening 2. During abstract screening 3. During the full-text screening 4. Non-English articles, articles with missing abstracts, notes, editorials 5. Document Type: Excluded (Book, Short survey, Letter, Retracted)	Generic reports related to blockchain technology without describing specific applications

The research aimed to provide a thorough and credible review of blockchain consensus mechanism security by adhering to these steps.

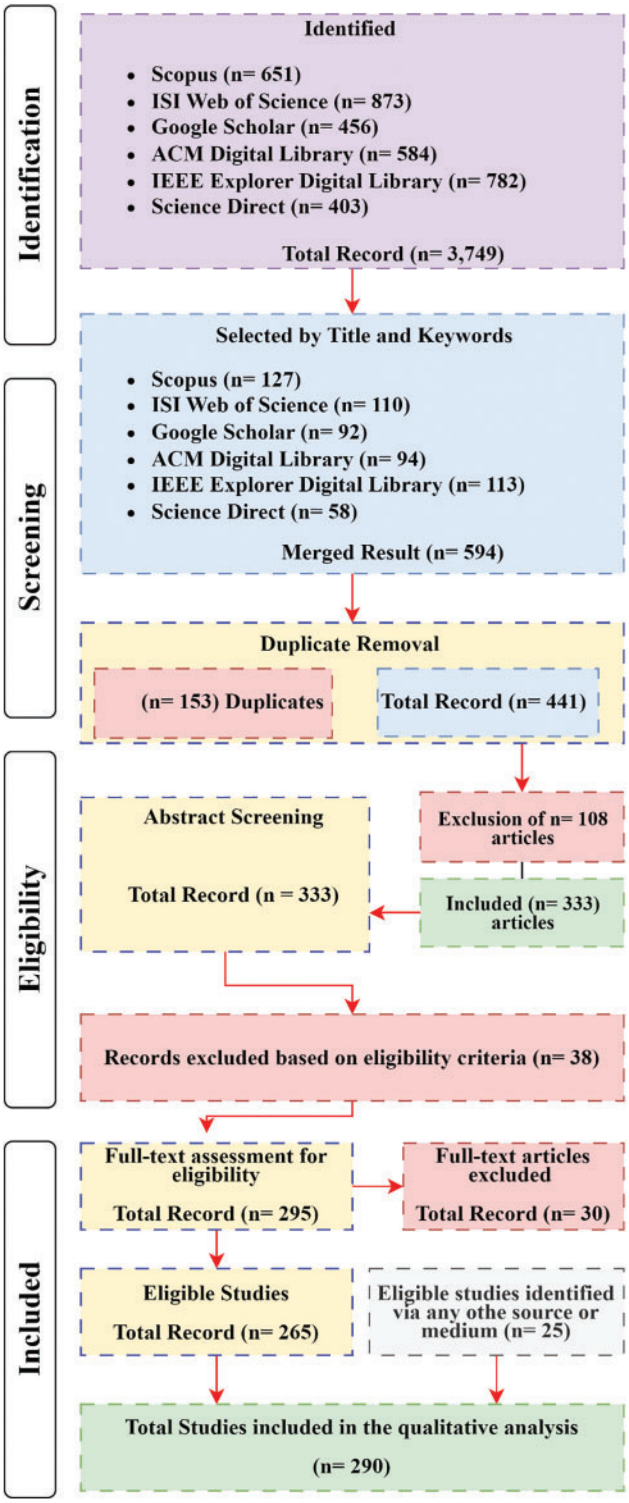
Identification
Identified
Scopus (n= 651)
ISI Web of Science (n= 873)
Google Scholar (n= 456)
ACM Digital Library (n= 584)
IEEE Explorer Digital Library (n= 782)
Science Direct (n= 403)
Total Record (n= 3,749)
Screening
Selected by Title and Keywords
Scopus (n= 127)
ISI Web of Science (n= 110)
Google Scholar (n= 92)
ACM Digital Library (n= 94)
IEEE Explorer Digital Library (n= 113)
Science Direct (n= 58)
Merged Result (n= 594)
Duplicate Removal
(n= 153) Duplicates
Total Record (n= 441)
Eligibility
Exclusion of n= 108 articles
Abstract Screening
Total Record (n = 333)
Included (n= 333) articles
Records excluded based on eligibility criteria (n= 38)
Included
Full-text assessment for eligibility
Total Record (n= 295)
Full-text articles excluded
Total Record (n= 30)
Eligible Studies
Total Record (n= 265)
Eligible studies identified via any othe source or medium (n= 25)
Total Studies included in the qualitative analysis
(n= 290)

Figure 2: Flowchart of the search strategy

4 Descriptive Analysis

The analysis involved reviewing and evaluating 3749 research papers published from January 2016 to February 2024, with grey literature excluded, resulting in a selection of 290 articles for descriptive analysis. This rigorous process ensured the inclusion of only peer-reviewed scholarly works, enhancing the reliability and validity of the findings. The descriptive analysis conducted on these articles serves three primary academic purposes:

Firstly, it provides valuable insights into current trends and developments in blockchain consensus mechanism security research. By systematically analyzing and synthesizing the content of these papers, the study identifies emerging patterns, gaps, and areas of consensus mechanism innovation within the academic discourse. This contributes to the ongoing scholarly conversation surrounding blockchain security, enabling researchers to build upon existing knowledge and address pressing challenges. Secondly, descriptive analysis helps visualize the diverse research approaches across various computer science disciplines in scholarly literature. Blockchain technology is inherently interdisciplinary, drawing upon fields such as cryptography, distributed systems, game theory, and economics [32]. By mapping out the selected papers' thematic areas and methodological approaches, the research gains a holistic understanding of the interdisciplinary nature of blockchain research and its implications for future advancements. Lastly, the descriptive analysis complements the overview of Consensus Mechanisms in Section II of the research paper. By contextualizing the findings within the broader framework of existing literature, the research validates and refines the theoretical underpinnings of their research. This ensures the analysis remains grounded in established knowledge while offering novel insights and perspectives to enrich the academic discourse. Two critical criteria were employed to classify the literature: (i) distribution of publications over time and thematic area, and (ii) distribution of publication types per year. This systematic approach allowed for a comprehensive examination of the evolving landscape of blockchain research and its implications for consensus mechanism security. The figures presented in the paper, such as Figs. 3 and 4, offer visual representations of the data, facilitating more straightforward interpretation and analysis. Fig. 3 illustrates a year-wise analysis of the selected papers, revealing a notable publication surge, particularly in 2019. This spike in research output reflects the growing interest and investment in blockchain technology and its applications. Despite roughly 2500 publications on blockchain-enabled applications until 2022, this figure escalated to nearly 3580 by 2023, highlighting the burgeoning nature of blockchain technology and academic interest. The research shows an increasing focus on blockchain security and energy efficiency, with 60% of papers published post-2019 reflecting the critical need for practical, sustainable consensus mechanisms.

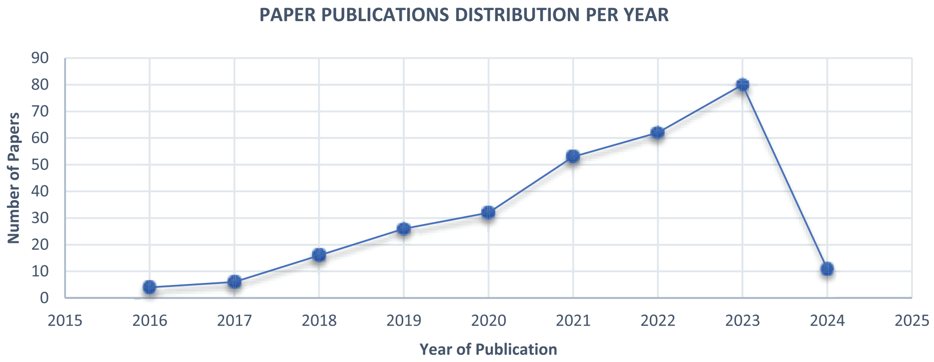

Figure 3: Number of papers by year of publication

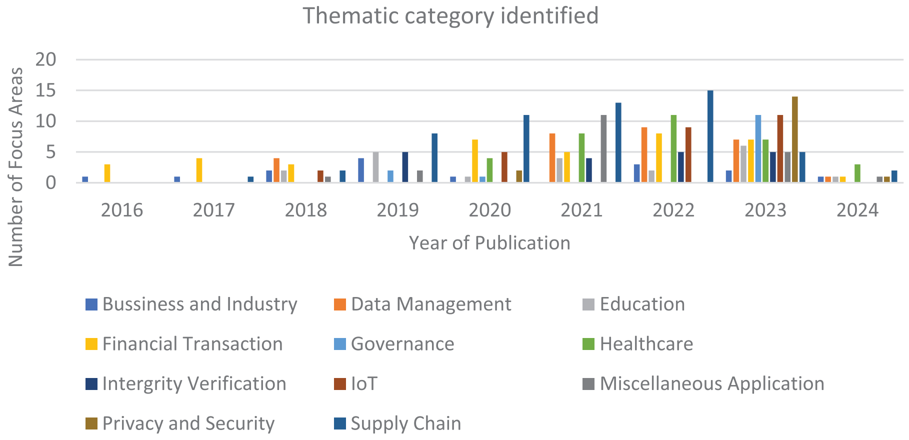

Figure 4: Research items based on the thematic category identified

Furthermore, the domain-specific distribution of the 290 research items over time, as depicted in Fig. 4, provides valuable insights into the focus areas within blockchain-based applications. Business-oriented applications emerge as a dominant theme, reflecting the widespread adoption of blockchain in various industries for purposes such as supply chain management, integrity verification, miscellaneous applications, etc. Supply chain, financial transaction, healthcare, IoT, and data management applications also garner significant attention, underscoring the multifaceted nature of blockchain technology and its potential to revolutionize diverse sectors.

Notably, while blockchain was initially synonymous with finance, the research community has yet to produce many financial-oriented applications. This discrepancy may be attributed to various factors, including regulatory challenges, technological limitations, and the need for further research and development in this domain. Additionally, the relatively high number of miscellaneous applications underscores the interdisciplinary potential of blockchain technology, highlighting its versatility and adaptability across a wide range of use cases.

In conclusion, the descriptive analysis offers valuable insights into the evolving landscape of blockchain consensus mechanism security research, providing researchers with a comprehensive understanding of current trends, challenges, and opportunities. By contextualizing the findings within the broader framework of existing literature, researchers can contribute to ongoing scholarly discourse, driving innovation and advancement in blockchain technology and its applications. Research shows a growing focus on blockchain consensus security and energy efficiency, with 60% of papers published post-2019. Hybrid consensus mechanisms, such as PoW/PoS, have improved scalability and security in blockchain applications. However, gaps in scalability, privacy, and interoperability hinder adoption. Future research should address these gaps through hybrid mechanisms and privacy-preserving techniques. Enhancing visuals and transparency and connecting blockchain advancements to broader tech trends can help policymakers and industry leverage blockchain's potential.

5 Consensus Mechanisms Security

This section presents the most common variants of consensus mechanisms and their security aspects. Consensus mechanisms are crucial in distributed ledgers where nodes must collectively agree on a valid version without central authority [3], as explained earlier. The research demonstrates consensus mechanisms' fundamental principles, operation, and vulnerabilities, mainly focusing on

PoW, PoS, DPoS, and PBFT algorithms and their susceptibility to attack vectors. In contrast, previous sections covered the need for blockchain consensus and its underlying theories. However, the dependence on consensus algorithms renders them vulnerable. Targeting these algorithms can compromise the security and integrity of the digital ledger, making them susceptible to attacks [33]. Therefore, this section will address such attacks.

5.1 Proof of Work

Various blockchain consensus algorithms exist, with proof of work being the original one introduced by Nakamoto for Bitcoin [1]. PoW is a consensus mechanism where miners compete to solve puzzles to validate transactions and add blocks to the blockchain [17]. PoW remains a robust and battle-tested consensus mechanism, and the emergence of alternative approaches reflects the ongoing quest for more efficient, secure, and sustainable blockchain networks. Consequently, alternative consensus algorithms have emerged to address these issues.

5.1.1 Inside PoW Mining

PoW mining aims to find a block with a hash below the difficulty threshold that contains only valid transactions. Miners manipulate block headers by adjusting the nonce value, exploiting the hash function's properties to produce diverse hashes [34]. The security of PoW depends on the robustness of the hash function, as faster hash computations confer advantages in block creation. Weaknesses in the hash function can compromise the security of PoW, highlighting the importance of secure hash functions in blockchain networks [35,36], as illustrated in Fig. 5 below.

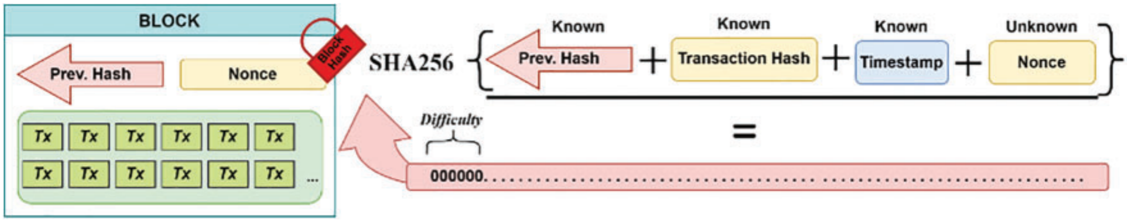

Figure 5: Inside PoW mining

5.1.2 Attacking PoW Consensus

The proof of work algorithm relies on security via scarcity but is vulnerable to various attacks if certain assumptions are violated. These include the hash function's security, appropriate difficulty setting, and most miners being honest [9]. Violating these assumptions can lead to attacks such as 51% attacks, Long-Range Attacks, Finney Attacks, Orphaned Blocks, Double-Spend Transactions, and Denial of Service (DoS) attacks [37]. The security of the PoW consensus algorithm used in blockchain systems is a crucial concern. Researches [38,39] both address the issue of security in the PoW protocol. A research study [38] focuses on the impact of long-delay attacks and proposes an optimized model to reduce the risk of data loss. Research [39] introduces the PoWs mechanism, which adjusts mining difficulty based on calculation force and coinage, thereby reducing the impact of mining pool nodes. Another research study [38,39] proposes strategies to enhance the security of the PoW consensus. The research of [40] suggests a zero-determinant strategy to alleviate miners' dilemma. At the same time, this paper [41] presents a hybrid PoW-PoS implementation to counter the 51% attack, ensuring a regular distribution of mining rewards. These studies collectively contribute to understanding and improving the PoW consensus algorithm.

The 51% Attack

A 51% attack exploits proof-of-work's majority vote system, allowing a malicious entity to control the blockchain. The attacker can replace the legitimate chain by controlling over half of the computational resources, enabling double-spend transactions. A 51% attack occurs when malicious entities control over half of a blockchain network's computational resources. With this majority control, the attacker can manipulate the blockchain by creating a longer chain, overriding legitimate transactions, and potentially executing double-spend transactions. The 51% attack is a substantial threat to Proof of Work (PoW) blockchains, where an attacker with over 50% of the network's hash power can influence the blockchain. These can lead to double-spending and other malicious activities [42]. To address this, a new technique has been proposed that combines the history-weighted information of miners with the total calculation difficulty, significantly increasing the cost of a traditional attack [42], as in Fig. 6.

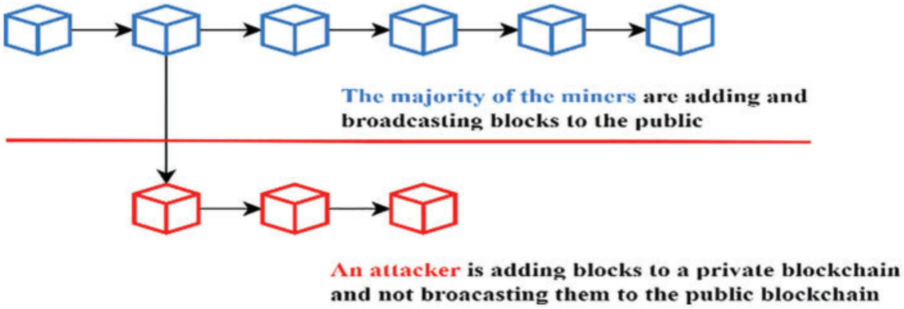
The majority of the miners are adding and broadcasting blocks to the public
An attacker is adding blocks to a private blockchain and not broacasting them to the public blockchain

Figure 6: 51% attack

However, the 51% attack is not limited to PoW blockchains, as it can also be exploited in Proof-of-Stake (PoS) systems, where the attacker needs to achieve 51% of the cryptocurrency [43]. To secure PoW ledgers, checkpointing has been suggested as a mechanism to protect against 51% of attacks [44]. Additionally, a new proof of work mechanism has been proposed to improve decentralization and reduce the risk of 51% attacks without increasing the risk of Sybil attacks [45].

Long-Range Attack

The Long-Range Attack vulnerability targets previously accepted blocks within the network to rewrite them. Attackers initiate this by generating a fork at a point preceding the current chain length, seeking to replace existing blocks. Detecting and preventing such assaults pose significant challenges [46]. Studies [47,48] underscore the persistence and targeted nature of attackers, with a focus on Secure Shell (SSH) brute-force attacks and on DDoS attacks. These findings imply that similar persistent and targeted strategies may be employed by attackers in long-range attacks on old blocks. Insights from [49] further illuminate these attacks. The research examines the significant volume and variety of non-productive traffic and analyzes the errors and pitfalls in the crowdsourcing process of ad-blocking systems. These studies suggest that attackers might exploit vulnerabilities in old blocks, such as misconfiguration and environmental factors, to generate a fork and disrupt the network.

Finney Attack

Named after Bitcoin developer Hal Finney, this vulnerability arises when an attacker mines a block with a transaction and quickly makes a payment to a merchant [50]. If the merchant accepts the payment before the block is confirmed, the attacker can replace the original block with a longer chain that excludes the transaction. In this attack, attacker A is a miner who issues a transaction T_A^A at a time $t_{T_A^A}$ to an account controlled by them and mines a block B_A containing that transaction. The attacker then keeps the mined block for himself and sends a transaction T_A^V to a seller V at a time $t_{T_A^V}$ As the block B_A was not published and the transaction T_A^A was not validated, V accepts the transaction T_A^V. Moreover, delivers the product to the attacker. After receiving the product, A publishes the block B_A containing the transaction T_A^A. Thus, as $t_{T_A^V} > t_{T_A^A}$, the network participants discard the transaction T_A^V, and V gains the product with remuneration. This way, the attacker gets the goods or services without paying [37,51,52].

Double-Spend Transactions

In PoW, a malicious actor could attempt to spend the same cryptocurrency twice by creating two conflicting transactions. If the attacker controls enough computational power, they can ensure that their double-spending transaction gets confirmed [53,54]. The vulnerability of PoW to double-spend attacks is a significant concern, with the likelihood and duration of such attacks being influenced by transaction recency and attacker computational power [55]. Introduce the whale attack, which incentivizes miners to collude and increases the likelihood of double spending. The research reviews various solutions to the double-spending problem, including the PoW and PoS consensus mechanisms, but notes their vulnerability to attacks. Akbar et al. [56] propose a reputation-based mechanism for preventing double spending without payment confirmations, highlighting the potential for innovative solutions.

Denial of Service (DoS)

A DoS attack can exploit flaws in the proof of work consensus algorithm by manipulating difficulty values, as shown in Fig. 7 below. If an attacker reduces network resources, the block creation rate decreases, leading to degraded blockchain performance and potential network downtime. This attack, alongside the 51% attack, undermines the decentralized nature of blockchain networks. Any proposed fixes for these attacks risk centralizing the network, contrary to the blockchain's intended design [57]. Many studies have explored the impact of Denial of Service (DoS) attacks on the proof-of-work consensus. The researches of [58,59] both propose control-based solutions to maintain consensus in multiagent systems despite DoS attacks. The work [58] focuses on distributed observer-based controllers while [59] introducing a switched system model and robust output consensus conditions. DoS attack frequency and duration [60] develops a distributed event-triggered control law for secure average consensus in the existence of DoS attacks. These studies collectively underscore the potential for control-based solutions to mitigate the impact of DoS attacks on consensus algorithms [61].

5.2 Proof of Stake

Proof of Stake (PoS) is a consensus mechanism used in cryptocurrency networks, where stakeholders with significant holdings validate transactions and create new blocks [62]. PoS is faster, cheaper, and more energy efficient than proof of work. While it carries a risk of centralization when a few stakeholders control a large portion of the currency, this is less likely in widely held currencies. PoS selects validators based on their stake in the network, rewarding them for their work. This model allows for faster transactions, reduced costs, and lower energy consumption than proof of work [63], as shown in Fig. 8 below.

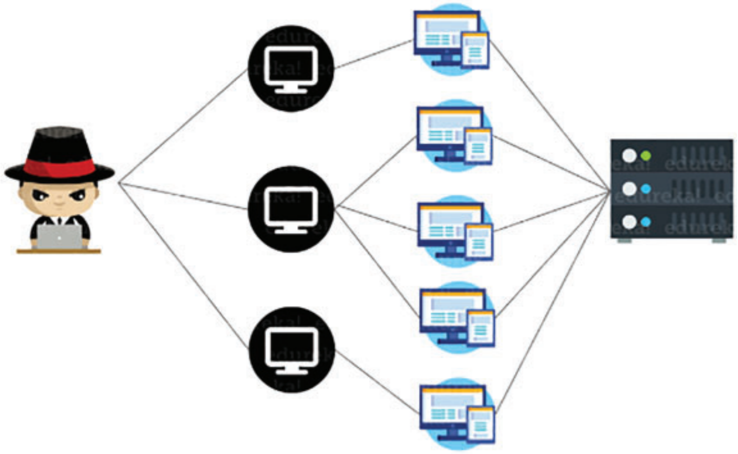

Figure 7: Denial of service attack

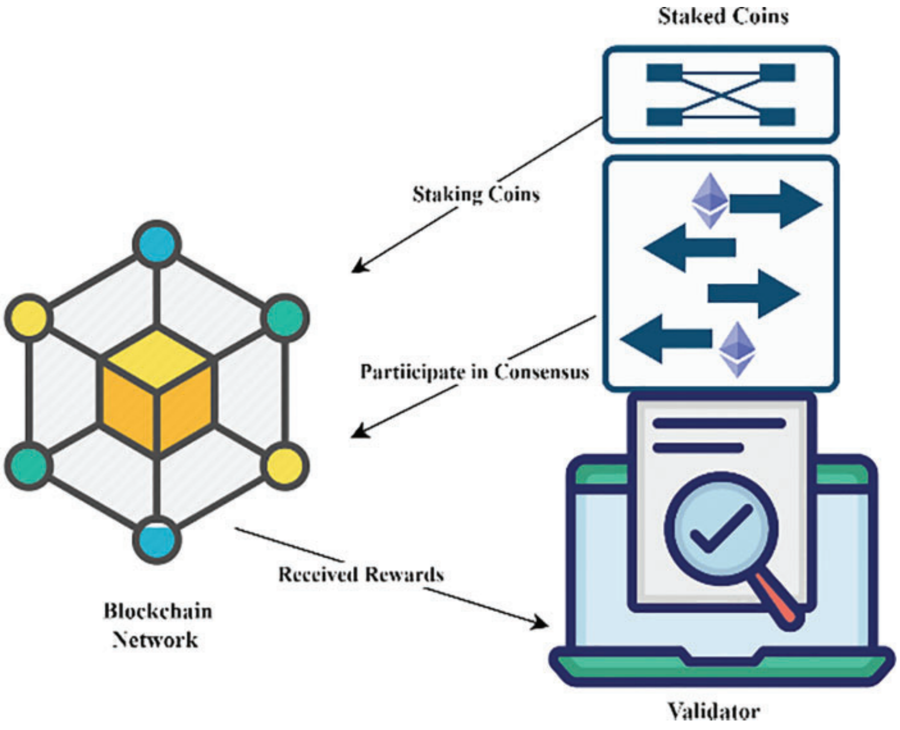

Figure 8: Proof of work

5.2.1 Choosing the Block Creator

Proof of Stake (PoS) determines who creates the next block in a distributed ledger based on stakeholders' cryptocurrency holdings, with higher holdings increasing the chance of selection [7,62]. Some variants cap the voting power of single accounts to prevent centralization, but anonymity allows holders to distribute their holdings across multiple accounts. A pseudo-random algorithm selects validators for each block based on the previous block's hash value, ensuring unpredictability while maintaining decentralization. Two main selection algorithms exist: direct stake-based and coin age-based, aiming to balance fairness and probability of selection. While PoS offers advantages over proof of work, its design and implementation are complex, as seen in Ethereum's transition delays. Various PoS variants exist, each with its security considerations [37], as in Fig. 9 below.

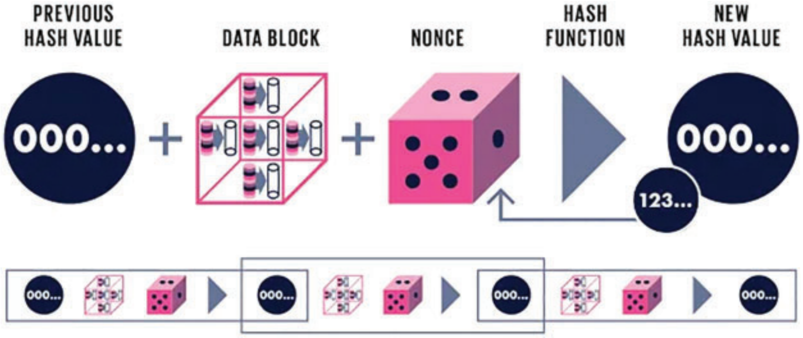

Figure 9: Choosing the block creator

5.2.2 *Attacking PoS Consensus*

While PoS offers advantages over proof of work, such as reduced computation and a lower probability of simultaneous block creation, it is susceptible to attacks. PoS relies on the scarcity of cryptocurrency ownership to prevent centralization. Flaws in the block creator selection process, such as broken hash functions or digital signature algorithms, can compromise PoS security [10,22,64]. This section will cover various attacks, including the XX% attack, fake stake attacks, long-range attacks, nothing-at-stake problems, and sour milk attacks.

XX% Attack and the PoS "Timebomb"

In PoS consensus algorithms, owning a significant portion of the cryptocurrency stake provides considerable power but only equates to complete control as in proof of work. The probability of being selected as the block creator is proportional to the stake owned. Short-term attacks, such as controlling multiple consecutive blocks, are possible with a high stake percentage [64]. However, in the long term, the "proof of stake time bomb" emerges, where the wealthiest stakeholder continually accumulates more stakes through rewards, eventually monopolizing the entire blockchain [65]. Thus, while not immediate, the possibility of complete control exists in PoS systems if a determined attacker continuously reinvests rewards into the stake.

Fake Stake Attacks

Fake stake attacks target Proof of Stake (PoS) systems by forcing blockchain nodes to allocate memory and CPU resources to validate a phony chain. Unlike Proof of Work (PoW), where validation is straightforward, PoS validation involves verifying block headers and contents, including stake transactions. This complexity makes PoS validation more resource-intensive [56]. Attackers can generate fake chains, causing nodes to download and validate them, consuming resources, and potentially slowing down the network. This denial of service attack exploits the most extended chain rule, disrupting the blockchain's operation by overwhelming nodes with fake chain validation [66].

Long-Range Attacks

The long-range attack targets PoS blockchains and exploits the longest-chain rule [67]. Initially owning some stake, the attacker builds a divergent blockchain alongside the main chain [67]. They strategically create blocks on their malicious chain while deliberately skipping block creation on the main chain. By reinvesting block rewards, the attacker's stake in the malicious chain proliferates over time, eventually allowing them to control all stakes and overtake the main chain [68]. This attack exploits natural or induced errors to accelerate the process. Once the attacker controls the longest chain, they can force its acceptance by the network, potentially preventing the blockchain. The time taken for this attack depends on the attacker's initial stake percentage, making its feasibility variable based on available resources [56]. As shown in the Fig. 10 below.

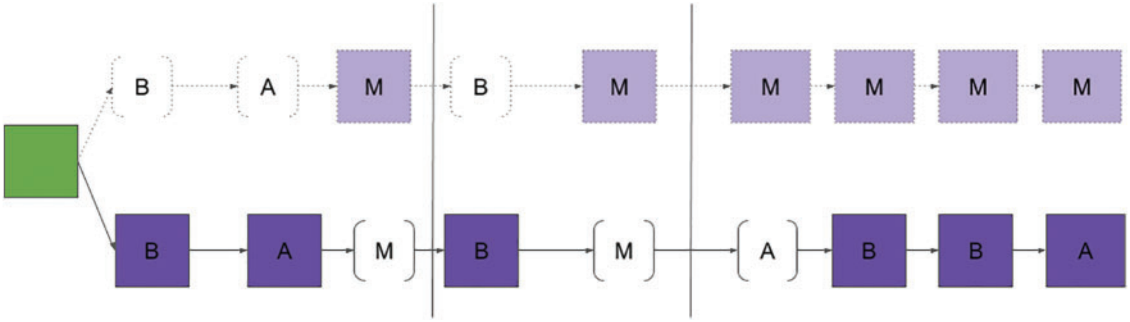

Figure 10: Long-term attacks described

Nothing at Stake Problem

The "nothing at stake" problem in blockchain emerges from misaligned incentives in proof-of-stake systems. While blockchain incentives are designed to reward proper behaviour, this problem occurs when block creators are presented with multiple versions of the blockchain. In the absence of safeguards, creators are incentivized to build on all chains to maximize their block rewards, as either chain could potentially become accepted as the legitimate one [62]. This behaviour poses challenges, such as making long-range attacks more feasible and causing participants to back legitimate and malicious chains to avoid losing rewards. While proof of stake systems can be designed to mitigate this problem, it remains a default issue where participants are inclined to support multiple chains to safeguard their rewards [69].

Censorship by Stake

The notion of "Censorship by Stake" underscores a pivotal concern within Delegate Proof of Stake (DPoS) systems, wherein concentrated ownership of stakes among a select group of validators wields disproportionate influence over network operations. This imbalance in stake distribution poses the imminent risk of censorship, whereby validators can potentially suppress transactions or disenfranchise specific participants from engaging with the network. Such wielded authority undermines the foundational tenets of decentralization and engenders a climate of exclusionary control [70,71].

Furthermore, Stake Grinding emerges as a complementary threat, further complicating the integrity of DPoS-based blockchain networks. Stake Grinding entails a nefarious tactic wherein malevolent entities manipulate the probabilistic selection process for block creation by surreptitiously altering their stake holdings or other pertinent parameters. Through systematically exploiting these variables, attackers can enhance their odds of being chosen as validators, thereby subverting the ostensibly random selection mechanism. The systematic pursuit of Stake Grinding compromises the integrity of the block validation process and precipitates a trajectory towards centralization, exacerbating the preexisting vulnerabilities within DPoS frameworks. Consequently, it is imperative to devise robust countermeasures to mitigate the harmful impacts of Censorship by Stake and Stake Grinding, thereby fortifying the decentralized ethos upon which DPoS networks are predicated [67].

Sybil Attacks

Sybil Attacks threaten the integrity and security of Proof of Stake (PoS) systems despite ongoing efforts to prevent them. In such attacks, malicious entities create multiple fake identities to gain disproportionate influence over the network, compromising its reliability and functionality [72]. Researchers have proposed various approaches to detect and mitigate Sybil attacks within PoS systems to address this issue. One proposed solution, suggested by the authors in [73], involves leveraging blockchain technology to track network nodes effectively. Utilizing the immutable and transparent nature of the blockchain makes it possible to verify the authenticity of network participants and detect any suspicious behaviour associated with Sybil attacks. Despite these proactive measures, recent researches [58,74] have shed light on a potential vulnerability in shard-based PoS blockchains. Some research findings [74] suggest that using Proof of Work (PoW) for identifier generation in shard-based PoS blockchains could exploit nodes with high hash power, allowing them to compromise the system's security. This underscores the importance of continued research and innovation in developing robust defenses against Sybil attacks in PoS systems. While various strategies have been proposed to mitigate Sybil attacks in PoS systems, ongoing research is essential to address emerging vulnerabilities and ensure the resilience of blockchain networks against such threats.

5.3 Delegated Proof of Stake (DPoS)

DPoS is a consensus mechanism in blockchain networks. This section explores its security vulnerabilities.

5.3.1 Centralization Tendency

DPoS involves the election of a limited number of delegates, also known as block producers, tasked with validating transactions and creating new blocks. This electoral system enhances scalability and efficiency but concurrently fosters centralization. With power concentrated in the hands of a select group of delegates, the decentralized nature of the network is jeopardized, posing potential security risks. The electoral process of delegates in DPoS significantly influences the decentralization trajectory of blockchain networks [37,75,76].

5.3.2 Vote Buying and Bribery

The DPoS consensus mechanism hinges upon the democratic voting process to elect delegates who play pivotal roles in transaction validation and block creation. However, this system is susceptible to the nefarious practices of vote buying and bribery, which undermine the integrity and fairness of the voting process. Vote buying occurs when delegates or candidates offer financial or otherwise incentives to stakeholders in exchange for their votes, skewing the democratic process in favour of the highest bidder. Similarly, bribery entails the provision of inducements or favours to voters or delegates in exchange for their allegiance or support [77].

The vulnerability to vote buying and bribery stems from the inherent nature of DPoS, where delegates with significant stakes wield considerable influence over the voting dynamics. As delegates with substantial holdings stand to gain from their election or re-election, they may resort to unethical means to secure votes, compromising the democratic principles of DPoS. Consequently, the voting process becomes susceptible to manipulation and coercion, leading to an inequitable power distribution among delegates and stakeholders within the blockchain network [78]. Researchers and developers have proposed various strategies and mechanisms to mitigate the risks associated with vote buying and bribery in DPoS systems to address these challenges. These include implementing transparent voting mechanisms, introducing penalties for engaging in fraudulent practices, and enhancing voter education and awareness programs to foster a more informed and resilient electorate. Additionally, cryptographic techniques and consensus algorithm design advancements may offer further avenues for safeguarding the integrity and fairness of the DPoS voting process, thereby promoting greater trust and confidence in decentralized governance mechanisms. of power [79].

5.3.3 51% Attack Risk

The DPoS consensus mechanism, characterized by a predetermined set of validators known as delegates, faces the looming threat of a 51% attack. This vulnerability arises when a malicious actor seizes control over more than half of the delegate positions within the network. In such a scenario, the attacker gains unprecedented authority to manipulate transactions and alter the blockchain's state, jeopardizing its integrity and security. While the likelihood of a 51% attack in DPoS is comparatively lower than in Proof of Work (PoW) systems, the risk remains palpable [9]. Despite the inherent susceptibility to 51% attacks, DPoS offers distinct advantages, such as expedited transaction processing and heightened energy efficiency when juxtaposed with PoW-based alternatives. However, striking a delicate equilibrium between bolstering security measures and enhancing scalability considerations in deploying DPoS-based blockchain networks is imperative. Achieving this balance necessitates a nuanced approach that acknowledges and mitigates the inherent vulnerabilities of DPoS while capitalizing on its efficiency-driven benefits. By prioritizing security and scalability imperatives, DPoS-based blockchains can aspire to foster robust and resilient ecosystems that thrive amidst the evolving landscape of blockchain technology [37].

5.4 Practical Byzantine Fault Tolerance (PBFT)

PBDT is an algorithm designed to achieve consensus in distributed systems even when some nodes exhibit Byzantine faults (i.e., behave arbitrarily or maliciously). While PBFT provides robustness, it's essential to understand its vulnerabilities:

5.4.1 Faulty Networks

The PBFT consensus protocol operates under the assumption of reliable communication channels, wherein all network participants can seamlessly exchange information without corruption. However, real-world network environments often exhibit vulnerabilities, wherein transmission channels may be susceptible to delivering corrupted packets. This inherent susceptibility introduces a significant risk factor, potentially compromising the integrity and functionality of the PBFT consensus mechanism. As such, mitigating strategies must be devised to address the ramifications of faulty networks, ensuring the robustness and resilience of PBFT-based blockchain networks in the face of adverse network conditions [80].

5.4.2 Disk Failures

In PBFT-based blockchain systems, disk failures represent a critical challenge due to their potential to corrupt, duplicate, lose, or fabricate information stored within disks. Given the pivotal role of data storage in maintaining the integrity and consistency of the blockchain ledger, PBFT consensus mechanisms must possess robust mechanisms for handling such failures gracefully. Failure to adequately address disk failures can compromise the blockchain network's reliability and trustworthiness, emphasizing the need for proactive measures to detect, mitigate, and recover from disk-related issues. As such, PBFT implementations must incorporate fault-tolerant strategies to safeguard against data corruption, duplication, loss, or falsification arising from disk failures, thereby ensuring the resilience and operational continuity of the blockchain system [81].

5.4.3 Node Impersonation

In PBFT-based blockchain systems, node impersonation poses a significant threat to the consensus process. Malicious nodes may attempt to impersonate legitimate nodes within the network, thereby disrupting the integrity and reliability of the consensus protocol. To mitigate this risk, PBFT mechanisms must incorporate robust detection and prevention mechanisms tailored to identify and thwart unauthorized node impersonation attempts. These mechanisms may include cryptographic authentication, digital signatures, and consensus rules designed to verify the identity and integrity of participating nodes. By implementing such measures, PBFT-based blockchain systems can enhance their resilience against node impersonation attacks, thereby preserving the trustworthiness and security of the consensus process [82].

5.4.4 Unauthorized Node Joining

The unauthorized joining of nodes within a PBFT-based cluster represents a potential security risk that can undermine the integrity and reliability of the consensus mechanism. When nodes join the cluster without proper authorization, they may introduce vulnerabilities and disrupt the consensus process. To address this threat, PBFT protocols must implement mechanisms for validating and authenticating new participants before granting them access to the network. These validation procedures may involve cryptographic authentication, identity verification, and consensus rules that only enforce authorized nodes' admission. By ensuring that only authorized nodes can join the cluster, PBFT-based systems can enhance their security posture and mitigate the risk of unauthorized access and malicious activity [83].

5.4.5 Unexpected Behavior

Unexpected behaviour, such as nodes operating when they shouldn't be due to factors like unexpected clock drift, poses a significant challenge to the reliability and security of PBFT-based systems. When nodes deviate from expected behaviour, it can disrupt the consensus process and undermine the integrity of the distributed system. PBFT protocols need to incorporate mechanisms to detect and mitigate such anomalies effectively [84]. By accounting for unexpected behaviour and implementing robust fault tolerance mechanisms, PBFT-based systems can enhance their resilience and ensure the integrity of the consensus process even in the face of unpredictable circumstances. Addressing these vulnerabilities is crucial for maintaining the robustness and security of PBFT-based systems, especially in real-world deployment scenarios where unexpected events are inevitable.

5.5 Additional Consensus Mechanisms

As blockchain technology evolves, various consensus mechanisms have emerged to address specific use cases and challenges. This section explores additional consensus mechanisms beyond conventional models like PoW and PoS. These alternative mechanisms offer unique approaches to achieving consensus and present their own set of advantages and vulnerabilities. By examining each mechanism in detail, we gain insight into their operation, security considerations, and potential applications within blockchain networks.

5.5.1 Proof of Authority (PoA)

PoA is a recently suggested permissioned blockchain BFT consensus protocol. It uses the longest-chain criterion to reach a consensus and depends on a group of reliable nodes to create blocks. However, because of its simplistic design, the protocol has problems with security and performance [85], such as:

Cloning Attacks

The Cloning Attack involves an attacker duplicating their Ethereum instance into two clones to communicate with different groups of sealers and potentially double-spend digital assets. The attacker creates two clones, each using the same public-private key pair, and exploits message delays to partition the network [86]. By copying blockchain content between clones and delaying message propagation, conflicting transactions can be issued to each sealer group. Success depends on influencing chain selection to discard the conflicting transaction branch, enabling double-spending. The attack is effective in both Aura and Clique PoA implementations, with varying success rates. Counter-measures to modify PoA protocols and improve security are proposed to prevent such attacks [87].

5.5.2 Proof of Space (PoSpace)

PoSpace is a consensus mechanism that utilizes the untapped storage capacity available on participants' devices to validate transactions and create new blocks. Although PoSpace offers energy efficiency, it also presents several security vulnerabilities that warrant consideration [3].

Resource Exhaustion

One significant security concern is resource exhaustion, where an attacker floods the network with excessive storage proofs [88]. This inundation of proofs can consume substantial network resources and significantly impact performance, potentially causing delays and disrupting the normal functioning of the blockchain network [5].

Collusion Attacks

Another security threat associated with PoSpace is collusion attacks, where validators conspire to manipulate storage proofs or control a significant portion of the network's storage space [89]. By doing so, they can compromise the integrity of the consensus process, potentially leading to double-spending or other malicious activities. Collusion attacks pose a significant risk to the security of PoSpace-based blockchain networks, highlighting the importance of robust security measures and vigilant monitoring to detect and prevent such malicious behaviour [5,88,90].

5.5.3 Proof of Elapsed Time (PoET)

PoET is a novel consensus algorithm used in blockchain networks to verify mining rights or select block validators. Unlike traditional PoW or PoS mechanisms, PoET leverages a *trusted execution environment (TEE) [37]*. In PoET, participating nodes compete for the right to validate transactions and create new blocks by independently choosing a random mining time. The node with the shortest chosen time becomes the validator for the next block. This process ensures fairness and decentralization in block validation. PoET relies on a TEE, providing a secure and isolated environment within a node's hardware to maintain the confidentiality of the chosen mining time until the designated waiting period elapses. Once the waiting time is over, the node can proceed with block validation, ensuring the reliability and security of the consensus process [91]. Despite its innovative approach, PoET is not without vulnerabilities:

TEE Compromises

The entire consensus process is at risk if the TEE is compromised (for example, due to a security flaw or malicious attack). An attacker gaining control over the TEE could manipulate the random selection process, leading to unauthorized block validation [91]. To address these vulnerabilities, PoET implementations must focus on enhancing TEE security. Regular audits, rigorous testing, and continuous examination are essential to maintaining the TEE's reliability. Additionally, diversifying the TEE providers and ensuring transparency in their operations can help prevent undue centralization [37,91].

5.5.4 Proof of Burn (PoB)

PoB is a distinctive consensus algorithm used in specific blockchain networks. It provides an alternative to conventional PoW or PoS mechanisms [92]. PoB introduces an innovative process where participants intentionally destroy existing coins to mint new ones. Initially, a participant triggers the process by transferring a certain amount of cryptocurrency from an existing wallet to an irretrievable address, signifying their dedication to the network by sacrificing value through coin-burning [69]. Consequently, participants who successfully execute coin burning gain the opportunity to engage in block validation and mining tasks, with their likelihood of being chosen as a validator increasing in correlation to the number of coins they burn [37]. Despite its unique approach, PoB entails several security considerations that merit attention:

Economic Loss

Participants risk losing valuable coins by burning them, introducing an economic aspect to the consensus process. This economic sacrifice can be considered a barrier to entry and may deter potential participants from engaging in PoB-based networks [37].

Sybil Attacks

A vulnerability inherent in PoB is the potential for Sybil attacks, where attackers create multiple identities to increase their influence within the network [92]. By burning coins across multiple identities, malicious actors can attempt to gain disproportionate control over the consensus process, compromising the network's integrity and decentralization [93]. Addressing these security concerns is crucial for ensuring the robustness and resilience of PoB-based blockchain networks. Implementing measures to mitigate economic risks and prevent Sybil attacks can help bolster the security and trustworthiness of PoB consensus mechanisms, enhancing their viability for real-world applications.

5.5.5 Proof of Identity (PoI)

PoI introduces a novel consensus algorithm that integrates real-world identity verification into the validation process, distinguishing it from traditional mechanisms like PoW or PoS. In PoI, participants undergo identity verification by providing government-issued identification, biometric data, or other personally identifiable information (PII) [94]. Verified participants gain eligibility to serve as validators within the network, tasked with confirming transactions, generating new blocks, and upholding the integrity of the blockchain [95]. Vulnerabilities include:

Privacy Concerns

Revealing personal information can compromise privacy. Requiring real-world identity verification raises privacy concerns. Participants may hesitant to share sensitive personal information, especially in a decentralized and pseudonymous environment [96]. The risk of exposing PII can compromise individuals' privacy.

Identity Theft

If an identity is stolen or impersonated, it affects the entire system's integrity. Malicious actors could exploit stolen identities to gain unauthorized access or manipulate the consensus process [96]. Remember that each consensus mechanism has trade-offs, and understanding their vulnerabilities is crucial for designing secure and efficient blockchain networks.

6 Security Considerations

Security considerations are paramount in evaluating the effectiveness and reliability of blockchain consensus mechanisms. As the backbone of blockchain networks, consensus mechanisms ensure the distributed ledger's integrity, immutability, and trustworthiness. Assessing the security features of each consensus mechanism involves a comprehensive analysis of their ability to withstand various attacks, maintain transaction finality, and handle adversarial models effectively.

One of the primary security considerations is resistance to attacks. This involves evaluating how well a consensus mechanism can defend against common threats such as double-spending, Sybil attacks, and 51% attacks. Understanding each mechanism's vulnerability to these attacks is crucial for determining its overall robustness and reliability in real-world scenarios [93]. Another critical aspect is finality, which refers to the certainty of transaction confirmations. Consensus mechanisms may offer probabilistic finality, where transactions are considered final after a certain number of confirmations, or deterministic finality, where transactions are guaranteed to be irreversible once they are included in the blockchain. Comparing the finality mechanisms of different consensus protocols helps assess their level of security and resilience against transaction reversals and other forms of tampering [97,98].

Furthermore, evaluating adversarial models is essential for understanding how consensus mechanisms handle Byzantine faults and malicious behaviour within the network. Byzantine fault tolerance (BFT) is a crucial concept in distributed systems, ensuring that the network can reach consensus even in the presence of malicious nodes. Consensus mechanisms need to be robust enough to detect and mitigate Byzantine faults effectively, preserving the integrity and security of the blockchain [3]. Table 4 shows the tabular representation of security considerations for various blockchain consensus mechanisms.

Table 4: Tabular representation of security considerations

Consensus mechanism	Resistance to attacks	Finality	Adversarial models
Proof of Work (PoW)	Vulnerable to 51% attacks, double-spending, Long-Range Attacks, Finney Attacks, Orphaned Blocks, and DoS attacks.	Probabilistic finality, based on the number of confirmations.	Byzantine fault tolerance is crucial for security. PoW relies on hash power to prevent attacks.
Proof of Stake (PoS)	Vulnerable to 51% attacks, fake stake attacks, long-range attacks, nothing-at-stake problems, censorship by stake, stake grinding, Sybil attacks.	Probabilistic finality, based on the number of confirmations.	Byzantine fault tolerance mechanisms are essential. PoS relies on stake ownership to secure the network.
Delegated Proof of Stake (DPoS)	Vulnerable to 51% attacks, centralization tendency, vote buying, and bribery.	Probabilistic finality, based on the number of confirmations.	Byzantine fault tolerance mechanisms are crucial. DPoS introduces centralization risks due to the delegate selection process.
Practical Byzantine Fault Tolerance (PBFT)	It is resistant to Byzantine faults but vulnerable to faulty networks, disk failures, node impersonation, unauthorized node joining, and unexpected behaviour.	Deterministic finality, where transactions are finalized once confirmed by a supermajority of nodes.	Focuses on Byzantine fault tolerance to ensure security. PBFT requires reliable communication and node integrity for robustness.
Proof of Authority (PoA)	Less resistant to censorship due to centralized authority nodes.	Probabilistic finality, based on the number of confirmations.	A centralized approach may compromise security.
Proof of Space (PoSpace)	Vulnerable to resource exhaustion attacks and collusion attacks.	Probabilistic finality, based on the number of confirmations.	Security relies on the integrity of storage space and the validation process.

(Continued)

Table 4 (continued)

Consensus mechanism	Resistance to attacks	Finality	Adversarial models
Proof of Elapsed Time (PoET)	Vulnerable to TEE compromises and centralization risks.	Probabilistic finality, based on the number of confirmations.	Relies on trusted execution environments for security. PoET introduces centralization risks due to TEE control.
Proof of Burn (PoB)	Vulnerable to economic loss, Sybil attacks.	Probabilistic finality, based on the number of confirmations.	Security relies on participants' willingness to burn coins for mining.
Proof of Identity (PoI)	Vulnerable to privacy concerns and identity theft.	Probabilistic finality, based on the number of confirmations.	Security relies on real-world identity verification. Privacy and identity protection are essential for security.

This table provides an overview of the security considerations associated with each consensus mechanism, including its vulnerability to different types of attacks, finality mechanisms, and how it handles adversarial models such as Byzantine faults. In summary, security considerations thoroughly evaluate each consensus mechanism's ability to resist attacks, provide transaction finality, and handle adversarial models. By assessing these aspects, stakeholders can make informed decisions about the suitability of different consensus mechanisms for specific applications and use cases, eventually enhancing the security and reliability of blockchain networks.

7 Applications and Use Cases across Industries

With its array of consensus mechanisms, blockchain technology demonstrates versatility across numerous domains, showcasing its potential in various applications. From finance to supply chain management, education, healthcare, the Internet of Things (IoT), governance, and beyond, blockchain's impact is pervasive [5]. In financial transactions, consensus mechanisms like PoW and PoS have revolutionized cryptocurrencies, offering decentralized and secure transaction capabilities [2]. Similarly, consensus mechanisms ensure transparency and traceability in supply chain management, fostering stakeholder trust [99]. Privacy-preserving mechanisms such as zero-knowledge proofs in the healthcare sector enhance data security and confidentiality [100,101]. For the Internet of Things (IoT), consensus mechanisms address scalability challenges while maintaining security standards [102,103]. Moreover, blockchain-based consensus mechanisms ensure transparency, accountability, and efficiency in governance, citizenship services, voting systems, and public sector operations [99,104,105]. Furthermore, blockchain facilitates secure credential verification and educational academic record management [106]. These diverse applications underscore the adaptability and potential of blockchain consensus mechanisms across various sectors and industries. As listed below.

7.1 Financial Transactions

Cryptocurrencies, one of the pioneering applications of blockchain technology, rely heavily on consensus mechanisms to facilitate secure and transparent financial transactions [41]. Two prominent consensus mechanisms, PoW and PoS, dominate the landscape, offering distinct advantages and considerations PoW [41,43,44], famously utilized in Bitcoin, operates on the principle of computational power, where miners compete to solve complex mathematical puzzles to validate transactions and create new blocks [63]. This process ensures network security by requiring significant computational resources and deterring malicious actors. Conversely, PoS, exemplified by Ethereum's transition to the Ethereum 2.0 version, presents an energy-efficient alternative by replacing computational power with stake-based validation [63]. In PoS systems, validators are selected based on the amount of cryptocurrency they hold and commit as collateral. This approach reduces energy consumption, addresses scalability concerns, and encourages broader participation in the consensus process. Understanding the trade-offs between PoW and PoS is crucial for designing resilient and efficient blockchain networks tailored to specific needs.

7.2 Supply Chain

Consensus mechanisms are vital in ensuring traceability and transparency within supply chain management systems powered by blockchain technology [99]. By leveraging blockchain's immutable ledger, supply chain stakeholders can effectively track goods' journeys from origin to destination, fostering transparency and accountability throughout the process. A range of consensus mechanisms can be employed to uphold data integrity and transparency in supply chains, thereby enhancing stakeholder trust [107]. For instance, Proof of Authority (PoA) can designate trusted entities responsible for validating and recording transactions within the supply chain network, ensuring that only authorized participants contribute to the consensus process [63,86,108]. Similarly, Proof of Stake (PoS) mechanisms can incentivize stakeholders with a vested interest in the supply chain's success to validate transactions and maintain the ledger's integrity [62,63]. Moreover, consensus mechanisms like PBFT can further enhance the resilience of supply chain networks by enabling swift and efficient agreement among network participants, even in the presence of malicious actors or faulty nodes [109,110]. Therefore, the strategic selection and implementation of consensus mechanisms tailored to supply chain requirements are essential for establishing a robust and transparent ecosystem that promotes trust and efficiency across the supply chain lifecycle [99,107]. Another research [111] explores the limitations of blockchain technology in IoT, including computational power, resource constraints, delays, scalability, storage capacity, latency, energy efficiency, complexity, accessibility, and security. It proposes a lightweight consensus mechanism (LC4IoT) to overcome these issues while maintaining the benefits of blockchain technology in the IoT use-case of a food supply chain.

7.3 Healthcare

Blockchain consensus mechanisms offer significant potential in the healthcare sector, particularly in ensuring the secure and private sharing of sensitive medical data among patients, healthcare providers, and researchers [81]. One essential application is leveraging privacy-preserving mechanisms to uphold patient confidentiality while enabling valuable data sharing for research and treatment purposes. For instance, zero-knowledge proofs (ZKPs) can validate transactions or assertions without revealing the underlying data, safeguarding patient privacy. Through ZKPs, healthcare providers can cryptographically prove the accuracy of medical records or treatment histories without disclosing sensitive information to unauthorized parties. Additionally, selective disclosure mechanisms enable patients to control the dissemination of their health data, allowing them to share specific information with authorized entities while keeping the rest confidential. By integrating these privacy-preserving consensus mechanisms into blockchain-based healthcare systems, stakeholders can foster a trusted environment for data exchange, facilitating collaborative research efforts, personalized treatment approaches, and improved patient outcomes [84,101]. Furthermore, the unchangeable nature of blockchain guarantees the integrity and auditability of medical records, improving transparency and accountability within the healthcare ecosystem [107]. As such, the strategic implementation of privacy-preserving consensus mechanisms holds immense promise in revolutionizing healthcare delivery while safeguarding patient privacy and data security.

7.4 Internet of Things (IoT)

The Internet of Things (IoT) landscape is characterized by the proliferation of interconnected devices generating substantial volumes of data, necessitating robust mechanisms for secure and efficient processing and storage [112]. Blockchain consensus mechanisms propose a promising solution to address the scalability and security challenges inherent in IoT networks. One key consideration lies in striking a balance between scalability and security, as the sheer scale of IoT deployments requires mechanisms capable of handling large transaction volumes without compromising network integrity [103]. DPoS and PBFT are two consensus mechanisms well-suited to meet these demands [76]. DPoS enables efficient transaction validation by delegating the consensus process to a select group of trusted delegates, thereby enhancing scalability while preserving network security [78,113]. Similarly, PBFT ensures robustness against Byzantine faults by involving nodes to reach a consensus on the validity of transactions through a series of message exchanges [109,114,115]. By leveraging these consensus mechanisms, IoT networks can achieve the scalability necessary to accommodate the growing number of connected devices while maintaining the security and integrity of data transmissions.

Furthermore, the immutable nature of blockchain enhances data integrity and auditability, providing a trusted framework for IoT deployments across various industries, including smart homes, industrial automation, and healthcare. As IoT continues to evolve, the strategic integration of blockchain consensus mechanisms will be instrumental in building resilient and secure IoT ecosystems capable of unlocking the full potential of connected devices while mitigating security risks and ensuring data privacy [116]. Integrating blockchain with IoT devices presents several challenges, primarily related to scalability and flexibility. Many connected IoT devices require a scalable and flexible blockchain infrastructure. Ensuring data reliability, scalability, and trustworthiness among these devices is crucial. Additionally, interoperability among blockchain participants and the need for lightweight consensus algorithms to efficiently manage IoT transactions further complicate integration efforts [117,118].

7.5 Integrity Verification

In today’s digital landscape, ensuring data integrity is paramount across various domains, ranging from digital documents and academic credentials to intellectual property rights [3]. Blockchain consensus mechanisms offer a robust solution for verifying data integrity by leveraging the inherent immutability of the blockchain ledger. By storing data in a tamper-proof and decentralized manner, blockchain guarantees that once information is documented, it cannot be changed or deleted without consensus from the network participants [119]. This feature makes blockchain particularly suitable for applications where maintaining the integrity and authenticity of data is critical. For example, in digital documents, blockchain can be used to timestamp and certify the authenticity of contracts, legal agreements, and sensitive records, providing a verifiable audit trail of document revisions and ensuring compliance with regulatory requirements. Similarly, blockchain-based credentialing systems enable the secure and transparent verification of academic qualifications and professional certifications, reducing the risk of credential deception and enhancing trust in educational and professional institutions [78]. Furthermore, blockchain technology can safeguard intellectual property rights by establishing a decentralized registry for patents, copyrights, and trademarks, enabling creators to assert ownership and protect their innovations from infringement. By harnessing blockchain consensus mechanisms, organizations and individuals can validate the integrity of their data, mitigate the risk of tampering and unauthorized modifications, and foster greater trust and transparency in digital transactions and information exchange. Like blockchain technology and multitasking, federated learning promotes security and trust in the metaverse. Consensus methods are essential to the integrity of blockchain-based systems in the Metaverse. But attacks against these systems, including Sybil or 51% attacks, can potentially jeopardize the blockchain's integrity and, consequently, the Metaverse [120].

7.6 Governance

Blockchain technology offers transformative potential in governance systems, revolutionizing citizenship services, public sector operations, and voting processes. By leveraging blockchain-based governance systems, governments can streamline administrative procedures, enhance transparency, and foster greater trust among citizens [104]. Consensus mechanisms such as PoA or DPoS play a pivotal role in facilitating secure and decentralized decision-making, thereby mitigating the risks associated with fraud and manipulation in governance processes [78,108]. For citizenship services, blockchain enables the creation of digital identity systems that provide secure and tamper-proof verification of citizenship status, residency, and other essential credentials [94]. This ensures that citizens can access government services and benefits efficiently while minimizing the risk of identity theft and fraudulent claims. In the public sector, blockchain-powered governance systems can optimize resource allocation, track budget expenditures, and improve service delivery through transparent and auditable processes [95]. Additionally, blockchain-based voting mechanisms offer a secure and verifiable platform for conducting elections, enabling citizens to cast their votes remotely while ensuring the integrity and confidentiality of the electoral process. By embracing blockchain consensus mechanisms, governments can establish resilient and accountable governance frameworks that empower citizens, enhance democratic participation, and drive positive socio-economic outcomes [78,106].

7.7 Education

Blockchain technology holds immense potential to transform the management and verification of academic credentials and certifications [106]. By harnessing blockchain-based systems, educational institutions can establish tamper-proof and transparent platforms for storing, managing, and verifying academic records, certificates, and diplomas [121–123]. Consensus mechanisms embedded within blockchain networks play a critical role in safeguarding the integrity and authenticity of educational credentials and mitigating the risks associated with credential fraud and misrepresentation [123]. Through consensus mechanisms such as PoW or PoS, educational institutions can ensure that academic records are securely recorded on the blockchain ledger, enabling seamless verification of students' qualifications and achievements [75]. Additionally, blockchain technology facilitates the creation of decentralized networks for lifelong learning verification, allowing individuals to securely access and share their educational credentials across various institutions and organizations. By leveraging blockchain consensus mechanisms, the education sector can establish robust and reliable systems for credential verification, thereby enhancing trust, transparency, and efficiency in academic record management.

7.8 Data Management

Blockchain technology offers a powerful solution for organizations seeking secure and immutable data storage and auditing capabilities [101]. Through blockchain consensus mechanisms, such as PoW or PoS, organizations can establish a robust and tamper-proof environment for managing critical data assets [55,66]. By leveraging blockchain, organizations can track the provenance of data, ensuring transparency and accountability throughout its lifecycle. Additionally, blockchain facilitates immutable data storage, preventing unauthorized modifications and enhancing data integrity. This capability is precious for industries with stringent compliance requirements, such as healthcare, finance, and supply chain management. Moreover, blockchain-based data management systems enable streamlined auditing processes, providing auditors with transparent and verifiable access to historical data records. Blockchain consensus mechanisms are pivotal in revolutionizing data management practices, offering organizations a reliable and secure platform for storage, auditing, and managing their data assets [27,98,101,119].

7.9 Miscellaneous Applications

Blockchain technology and versatile consensus mechanisms facilitate various innovative applications across diverse domains. Smart contracts represent a prominent application, enabling automated and trustless execution of agreements on the blockchain. By leveraging consensus mechanisms like PoA or DPoS, smart contract platforms ensure the integrity and security of contractual transactions, offering a reliable solution for businesses seeking efficient contract execution [5]. Decentralized finance (DeFi) is another significant application empowered by blockchain consensus mechanisms. DeFi platforms leverage decentralized networks and smart contracts to provide financial services, including borrowing, lending, and trading, without traditional intermediaries. Consensus mechanisms like PoS or PoW underpin the security and reliability of DeFi protocols, ensuring transparent and efficient financial transactions [124].

Furthermore, blockchain-based gaming platforms are revolutionizing the gaming industry by introducing secure and transparent ownership of in-game assets. Through consensus mechanisms such as PoA or PoST, gaming platforms enable players to securely trade, transfer, and monetize their digital assets within the gaming ecosystem. This decentralized approach to gaming fosters player autonomy and ownership while also enhancing the overall gaming experience [125]. Blockchain consensus mechanisms unlock many possibilities across smart contracts, decentralized finance, and gaming applications, paving the way for innovative solutions that redefine traditional paradigms and empower users with greater control and security over their digital interactions. These use cases highlight the versatility of blockchain technology and its consensus mechanisms in addressing diverse challenges across different industries and sectors. It provides secure, transparent, and decentralized solutions; blockchain has the potential to revolutionize various aspects of modern society. By using blockchain, sensitive data can be shared securely among 5G stakeholders without compromising privacy, thanks to cryptographic techniques and secure data storage solutions [126]. The authors highlight blockchain's potential in 5G networks but acknowledge challenges such as scalability, performance, standardization, resource constraints, security, and infrastructure costs, highlighting the need for further research to ensure safe deployment.

8 Open Challenges and Future Directions

As blockchain technology progresses, researchers and developers actively explore avenues to improve blockchain networks' efficiency, scalability, security, and sustainability. One significant area for further investigation is enhancing scalability without compromising decentralization. Solutions such as sharding, layer-two protocols, and off-chain scaling techniques hold promise in addressing the scalability challenges faced by blockchain networks [4]. Additionally, advancing consensus mechanisms to achieve greater energy efficiency and environmental sustainability remains a key focus. Innovations in consensus algorithms, including hybrid approaches and energy-efficient protocols, are being researched to minimize the carbon footprint associated with blockchain operations [115]. Furthermore, ensuring robust security against emerging threats, such as quantum computing, requires ongoing research and development efforts to fortify cryptographic primitives and defense mechanisms. Moreover, improving interoperability and standardization across diverse blockchain platforms is essential for promoting seamless integration and collaboration within the blockchain ecosystem. By addressing these challenges and pursuing innovative solutions, the future of blockchain technology holds immense potential for transformative applications across various industries. Here are some proposed areas for further investigation and development.

8.1 Hybrid Mechanisms

Combining PoW and PoS, hybrid consensus mechanisms aim to leverage the strengths of both PoW and PoS while mitigating their respective weaknesses, striving for enhanced scalability, energy efficiency, and security [62,127,128]. Numerous studies have delved into the potential of hybrid consensus mechanisms, combining PoW and PoS to improve scalability, energy efficiency, and security. For instance, Reference [129] proposes Proof of Majority (PoM), a consensus algorithm that curtails energy wastage and fortifies security in private blockchain systems. Some research [62] shed light on PoW's drawbacks, including energy inefficiency and security vulnerabilities, advocating for PoS in forthcoming blockchain networks. A hybrid consensus algorithm incorporating locational marginal pricing for energy applications was introduced [128], aiming to address vulnerabilities inherent in both PoW and PoS, nothing-at-stake vulnerability issues in PoS. Additionally, Reference [130] outlines potential scenarios for transitioning from PoW to PoS, emphasizing the necessity of more energy-efficient consensus algorithms. These studies collectively underscore the potential of hybrid mechanisms in remedying the limitations of PoW and PoS. Hybrid consensus mechanisms combine Proof of Work (PoW) and Proof of Stake (PoS) to enhance scalability, reduce energy consumption, and improve network security. PoW's robust security relies on computational work, while PoS reduces this by allowing validators to validate blocks based on cryptocurrency holding. This combination would ensure a decentralized, resilient blockchain ecosystem for financial transactions [124], healthcare [127], and supply chain [131].

8.2 Quantum-Resistant Consensus

Preparing for Quantum Computing Threats, the emergence of quantum computing, and traditional cryptographic algorithms used in blockchain networks may become vulnerable to attacks. Future research will focus on developing quantum-resistant consensus mechanisms and cryptographic protocols to withstand quantum threats and ensure the longstanding security of blockchain systems [132,133]. The emergence of quantum computing poses a major threat to the security of blockchain systems, particularly in terms of their cryptographic protocols [134]. To address this, there is a need to develop quantum-resistant consensus mechanisms and cryptographic protocols [135]. One potential solution is the integration of quantum properties into the blockchain, such as using quantum key distribution and quantum synchronization [136], in application areas like Metaverse [120], and healthcare electronic systems [101]. Another approach is adopting post-quantum consensus solutions, which can enhance the security and resilience of blockchain systems [137], in some integrity verification systems [119].

8.3 Decentralized Governance

Research on decentralized governance in blockchain networks has highlighted the role of consensus mechanisms in decision-making, protocol upgrades, and dispute resolution [138]. These mechanisms, such as PoW, PoS, and PBFT, are crucial in redefining and challenging traditional democratic norms [139]. The concept of decentralized network governance, which is based on regulating power relationships in the digital domain, has been proposed as a new mode of governance [140]. This governance model, which includes decentralized autonomous organizations (DAOs), aims to ensure fairness, transparency, and inclusivity in decision-making processes [138]. Role of Consensus in Blockchain Governance, these mechanisms are crucial in decentralized networks' decision-making, protocol upgrades, and dispute resolution. Future research will explore innovative approaches to decentralized governance, including liquid democracy, quadratic voting, and decentralized autonomous organizations (DAOs), to ensure fairness, transparency, and inclusivity in blockchain governance [104].

8.4 Scalability Solutions

Improving Transaction Throughput, as blockchain networks face scalability and transaction throughput challenges, future research will focus on developing scalable consensus mechanisms and layer two scaling solutions. Techniques such as sharding, state channels, and sidechains will be explored to increase network capacity and reduce congestion [4,103].

Open challenges and future directions regarding scalability in blockchain applications across various industries include addressing the high transaction throughput required in supply chains [141] and financial transactions [124], which demands efficient handling of vast amounts of data and quick processing times. In healthcare [81], ensuring scalable and secure patient data management is crucial, while IoT [118] integration necessitates handling numerous interconnected devices with minimal latency. Governance applications require robust, scalable frameworks to manage large-scale, decentralized decision-making processes [104]. Data management must focus on scalable storage solutions to handle growing data volumes without compromising security or performance [142]. Future research should explore innovative consensus mechanisms, layer 2 scaling solutions, and cross-chain interoperability to meet these diverse scalability needs effectively.

8.5 Privacy-Preserving Mechanisms

The potential for privacy breaches in sensitive domains like healthcare and finance underscores the need for privacy-preserving consensus mechanisms in blockchain [143]. Various methods have been proposed to address this, including using threshold signatures to ensure data correctness and applying privacy-preserving solutions based on crypto-privacy techniques [100]. Consensus algorithms play a crucial role in maintaining the integrity and security of blockchain [144]. Using these algorithms in combination with privacy-preserving techniques is a crucial area for future research [145]. Also, Techniques like homomorphic encryption and secure multi-party computation need further development. Balancing data utility and privacy is crucial in big data analytics and AI-driven healthcare solutions [142].

8.6 Balancing Transparency with Confidentiality

While blockchain offers transparency and immutability, privacy concerns remain challenging, particularly in sensitive domains like healthcare and finance. Future research will explore privacy-preserving consensus mechanisms, zero-knowledge proofs, and secure multiparty computation techniques to enable confidential transactions while maintaining the truthfulness of the blockchain [40,95,100,101].

Balancing transparency and confidentiality in the food supply chain is crucial for food safety, quality assurance, and consumer trust. Blockchain technology can enhance transparency but must be combined with advanced cryptographic techniques for data protection [105,111,146]. Future research should focus on scalable algorithms and standardized protocols.

8.7 Interoperability Solutions

Consensus across Heterogeneous Blockchains achieving interoperability between different blockchain networks is essential for seamless data exchange and collaboration. The need for interoperability between diverse blockchain ecosystems is a pressing issue, with various solutions being explored. Researches [59,78] both provide comprehensive surveys of the current progress in this area, highlighting the complexity and challenges involved. The research proposes specific solutions, focusing on architectural approaches and introducing a new consensus protocol, Multi-tokens Proof of Stake (MPoS), for blockchain interoperability. These studies collectively underscore the importance of achieving interoperability and the ongoing efforts to address this critical need. Developing unified standards and ensuring compatibility among heterogeneous systems is crucial. Edge computing faces challenges in integrating diverse devices, platforms, and protocols for efficient data processing and communication [4,147]. Future research will focus on developing interoperability protocols, cross-chain communication standards, and interoperable consensus mechanisms to enable frictionless interaction between diverse blockchain ecosystems [59,78].

8.8 Energy Efficiency

Research has explored alternative consensus mechanisms to reduce blockchain energy consumption, such as Proof of Stake (PoS) and Proof of Authority [148]. These mechanisms aim to address the environmental impact of blockchain, with PoS being particularly effective in reducing energy consumption [149]. Other proposals, such as Proof of Contribution (PoC), have also been suggested to increase mining efficiency and reduce energy consumption [35]. However, the energy footprint of PoS-based systems can still vary significantly, with permissionless systems potentially having a larger energy footprint [149]. Therefore, while these alternatives promise to reduce energy consumption, further research is needed to understand their environmental impact fully. While PoW consensus provides robust security, its energy-intensive nature has raised concerns about sustainability and environmental impact. Future research will explore alternative consensus mechanisms, such as Proof of Stake, Proof of Authority, and energy-efficient PoW variants, to reduce blockchain's carbon footprint and promote sustainable development [44,51,56,72].

8.9 Formal Verification

Ensuring the correctness of consensus algorithms [13] emphasizes the importance of performance and efficiency in consensus algorithms while Reference [150] discusses the use of formal methods to ensure the security and reliability of blockchain consensus protocols. Also, Reference [22] provides an overview of basic consensus mechanisms and their evaluation and Reference [151] proposes a Secure and Trustworthy Blockchain-based Crowdsourcing (STBC) consensus protocol, verified using formal methods. These studies underscore the significance of formal verification techniques in ensuring consensus algorithms' correctness and security properties in blockchain technology. Formal verification techniques enable mathematical proofs of consensus algorithms' correctness and security properties. Future research will focus on applying formal methods, model checking, and theorem proving to rigorously analyze and verify the correctness of blockchain consensus mechanisms, ensuring robustness and reliability [106,119].

9 Conclusion Remarks

This systematic literature review (SLR) provides a comprehensive overview of blockchain consensus mechanisms, focusing on their security considerations, applications, open issues, and future directions. Consensus mechanisms are crucial for ensuring blockchain networks' integrity, reliability, and decentralization. The review highlights the security features and vulnerabilities of prominent consensus mechanisms such as PoW, PoS, DPoS, and PBFT. The review also explores real-world applications and use cases where blockchain consensus mechanisms excel, such as supply chain management, financial transactions, healthcare, and governance. Despite significant progress in blockchain research and development, several open issues and challenges persist, such as scalability, privacy, interoperability, energy efficiency, and formal verification. Future directions in blockchain consensus mechanisms aim to explore hybrid approaches, quantum-resistant solutions, decentralized governance models, scalability enhancements, privacy-preserving mechanisms, interoperability solutions, energy-efficient alternatives, and formal verification techniques. By advancing research in these areas, the blockchain community can overcome existing limitations, unlock new opportunities, and realize the full potential of decentralized systems.

In conclusion, this SLR provides valuable insights into the security, applications, challenges, and future directions of blockchain consensus mechanisms, contributing to the ongoing discourse on blockchain technology and governance. By building on the findings, researchers and practitioners can continue innovation, promote collaboration, and shape the future of decentralized systems and applications. Additionally, integrating blockchain with emerging technologies like IoT, AI, and quantum computing will open new avenues for research and development, driving the evolution of more robust, efficient, and secure decentralized networks. This SLR is a foundation for future studies and guides policymakers and industry stakeholders in making informed decisions in deploying and governance blockchain technologies. The ongoing collaboration and interdisciplinary research efforts are essential to address blockchain's complexities and dynamic challenges, ensuring its sustainable and transformative impact across various sectors. Research highlights blockchain consensus security and energy efficiency, with 60% of papers post-2019. Hybrid mechanisms improve scalability and security, but gaps in privacy and interoperability hinder adoption.

Acknowledgement: The authors would like to thank the Yayasan Universiti Teknologi PETRONAS: Pre-Commercialization Research Grant for funding this project. The grant title is Assessment of Structural Steel Riser-Guard Load Capacities on the Resultant Impact on Offshore Structures Loading.

Funding Statement: The above research is funded by Universiti Teknologi PETRONAS and grants (YUTP-PRG: 015PBC-011).

Author Contributions: The authors confirm the contribution to the paper as follows: study conception: Muhammad Muntasir Yakubu, Aisha Zahid Junejo, and Muhammed Siraj; data collection, analysis,

and writing. Mohd Fadzil B Hassan, Kamaluddeen Usman Danyaro, Aisha Zahid Junejo, Saidu Yahaya, Kamal Abdussalam, and Shamsuddeen Adamu did revisions. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The authors confirm that the data supporting this study's findings are available within the article.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

Supplementary Materials: The supplementary material is available online at https://doi.org/10.32604/csse.2024.054556.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," in *White Paper*, 2008. Accessed: Jul. 24, 2024. https://assets.pubpub.org/d8wct41f/31611263538139.pdf

[2] A. S. Yadav, N. Singh, and D. S. Kushwaha, "Evolution of blockchain and consensus mechanisms & its real-world applications," *Multimed. Tools Appl.*, vol. 82, no. 22, pp. 34363–34408, 2023. doi: 10.1007/s11042-023-14624-6.

[3] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. 9, pp. 43620–43652, 2021. doi: 10.1109/ACCESS.2021.3065880.

[4] J. P. Queralta and T. Westerlund, "Blockchain for mobile edge computing: Consensus mechanisms and scalability," in *Mobile Edge Computing*. Cham: Springer, 2021, pp. 333–357. doi: 10.1007/978-3-030-69893-5_14.

[5] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020. doi: 10.1109/COMST.2020.2969706.

[6] A. K. Yadav, K. Singh, A. H. Amin, L. Almutairi, T. R. Alsenani and A. Ahmadian, "A comparative study on consensus mechanism with security threats and future scopes: Blockchain," *Comput. Commun.*, vol. 201, no. 2, pp. 102–115, 2023. doi: 10.1016/j.comcom.2023.01.018.

[7] W. Wang *et al.*, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.

[8] X. Fu, H. Wang, and P. Shi, "A survey of blockchain consensus algorithms: Mechanism, design and applications," *Sci. China Inf. Sci.*, vol. 64, pp. 1–15, 2021.

[9] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Appl. Sci.*, vol. 9, no. 9, 2019, Art. no. 1788.

[10] M. Baboi, "Security of consensus mechanisms in blockchain," *Rom. Cyber Secur. J.*, vol. 5, no. 2, pp. 45–53, 2023. doi: 10.54851/v5i2y202305.

[11] S. J. Alsunaidi and F. A. Alhaidari, "A survey of consensus algorithms for blockchain technology," in *2019 Int. Conf. Comput. Inf. Sci. (ICCIS)*, IEEE, 2019, pp. 1–6.

[12] M. Borse, P. Shendkar, Y. Undre, A. Mahadik, and R. Y. Patil, "A review of blockchain consensus algorithm," in *Expert Clouds and Applications*, 2022, vol. 444, pp. 415–426. doi: 10.1007/978-981-19-2500-9_31.

[13] J. Yusoff, Z. Mohamad, and M. Anuar, "A review: Consensus algorithms on blockchain," *J. Comput. Commun.*, vol. 10, no. 9, pp. 37–50, 2022.

[14] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, 2021. doi: 10.1136/bmj.n71.

[15] R. Sarkis-Onofre, F. Catalá-López, E. Aromataris, and C. Lockwood, "How to properly use the PRISMA Statement," *Syst. Rev.*, vol. 10, pp. 1–3, 2021. doi: 10.1186/s13643-021-01671-z.

[16] N. Chaudhry and M. M. Yousaf, "Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities," in *2018 12th Int. Conf. Open Source Syst. Technol. (ICOSST)*, IEEE, 2018, pp. 54–63.

[17] P. Zhang, D. C. Schmidt, J. White, and A. Dubey, "Consensus mechanisms and information security technologies," *Adv. Comput.*, vol. 115, pp. 181–209, 2019. doi: 10.1016/bs.adcom.2019.05.001.

[18] H. Xiong, M. Chen, C. Wu, Y. Zhao, and W. Yi, "Research on progress of blockchain consensus algorithm: A review on recent progress of blockchain consensus algorithms," *Future Internet*, vol. 14, no. 2, 2022, Art. no. 47. doi: 10.3390/fi14020047.

[19] S. Zhou, K. Li, L. Xiao, J. Cai, W. Liang and A. Castiglione, "A systematic review of consensus mechanisms in blockchain," *Mathematics*, vol. 11, no. 10, 2023, Art. no. 2248. doi: 10.3390/math11102248.

[20] R. Jain, P. Borkar, P. Deshmukh, S. Badhiye, K. Nimje and K. Gupta, "Choosing a suitable consensus algorithm for blockchain applications: A review of factors and challenges," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 10s, pp. 333–341, 2024.

[21] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics Inform.*, vol. 36, no. 7674, pp. 55–81, 2019. doi: 10.1016/j.tele.2018.11.006.

[22] X. Han and Y. Liu, "Research on the consensus mechanisms of blockchain technology," *Netinfo Secur.*, vol. 5, no. 9, pp. 147–152, 2017.

[23] W. Yao, J. Ye, R. Murimi, and G. Wang, "A survey on consortium blockchain consensus mechanisms," 2021, *arXiv:2102.12058.*

[24] A. Nick and L. Hoenig, "Consensus mechanisms in blockchain technology," *Lexology*, 2020. Accessed: Jul. 24, 2024. [Online]. Available: https://www.lexology.com/library/detail.aspx

[25] F. Saleh, "Blockchain without waste: Proof-of-stake," *Rev. Financ. Stud.*, vol. 34, no. 3, pp. 1156–1190, 2021. doi: 10.1093/rfs/hhaa075.

[26] V. Gramoli, "From blockchain consensus back to Byzantine consensus," *Future Gener. Comput. Syst.*, vol. 107, no. 3, pp. 760–769, 2020. doi: 10.1016/j.future.2017.09.023.

[27] C. Zhang, C. Wu, and X. Wang, "Overview of blockchain consensus mechanism," in *Proc. 2020 2nd Int. Conf. Big Data Eng.*, 2020, pp. 7–12.

[28] T. Thanujan, R. Rajapakse, and D. Wickramaarachchi, "A review of blockchain consensus mechanisms: State of the art and performance measures," in *KDUIRC 2020 13th Int. Res. Conf.*, Ratmalana, Sri Lanka, 2020, pp. 315–326. doi: 10.1007/978-3-030-03035-3.

[29] F. Aponte, L. Gutierrez, M. Pineda, I. Meriño, A. Salazar and P. Wightman, "Cluster-based classification of blockchain consensus algorithms," *IEEE Lat. Am. Trans.*, vol. 19, no. 4, pp. 688–696, 2021. doi: 10.1109/TLA.2021.9448552.

[30] J. S. Gans and R. T. Holden, *Mechanism Design Approaches to Blockchain Consensus*. National Bureau of Economic Research, 2022. Accessed: Jul. 24, 2024. [Online]. Available: http://www.nber.org/papers/w30189

[31] B. Kitchenham and S. Charters, *Guidelines for Performing Systematic Literature Reviews in Software Engineering*, 2007. Accessed: 08 Aug. 2014. [Online]. Available: https://www.cs.auckland.ac.nz/~norsaremah/2007%20Guidelines%20for%20performing%20SLR%20in%20SE%20v2.3.pdf

[32] B. Cao *et al.*, "Blockchain systems, technologies, and applications: A methodology perspective," *IEEE Commun. Surv. Tut.*, vol. 25, no. 1, pp. 353–385, 2022. doi: 10.1109/COMST.2022.3204702.

[33] Z. Painter, V. Cook, C. Peterson, and D. Dechev, "Descriptor based consensus for blockchain transactions," in *Proc. 15th ACM Int. Conf. Distrib. Event-Based Syst.*, 2021, pp. 114–125.

[34] I. G. A. K. Gemeliarana and R. F. Sari, "Evaluation of proof of work (POW) blockchains security network on selfish mining," in *2018 Int. Seminar Res. Inf. Technol. Intell. Syst. (ISRITI)*, 2018, pp. 126–130.

[35] T. Xue, Y. Yuan, Z. Ahmed, K. Moniz, G. Cao and C. Wang, "Proof of contribution: A modification of proof of work to increase mining efficiency," *2018 IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 1, pp. 636–644, 2018. doi: 10.1109/COMPSAC.2018.00096.

[36] S. Lv, H. Li, H. Wang, and X. Wang, "CoT: A secure consensus of trust with delegation mechanism in blockchains," in *Blockchain Technol. Appl.: Second CCF China Blockchain Conf., CBCC 2019*, Chengdu, China, Springer, 2020, pp. 104–120.

[37] G. A. F. Rebello, G. F. Camilo, L. C. Guimaraes, L. A. C. de Souza, G. A. Thomaz and O. C. M. Duarte, "A security and performance analysis of proof-based consensus protocols," *Ann. Telecommun.*, vol. 77, no. 7–8, pp. 1–21, 2022. doi: 10.1007/s12243-021-00896-2.

[38] T. Feng and Y. Liu, "Optimized model analysis of blockchain PoW procotol under long delay attack," in *Proc. 2023 2nd Asia Conf. Algorithms Comput. Mach. Learn.*, 2023, pp. 25–30.

[39] K. Sui, C. Yang, and Z. Li, "Research on consensus mechanism for anti-mining concentration," in *Communications, Signal Processing, and Systems*. Singapore: Springer, 2020, pp. 483–492.

[40] Y. Zhen, M. Yue, C. Zhong-yu, T. Chang-bing, and C. Xin, "Zero-determinant strategy for the algorithm optimize of blockchain PoW consensus," in *2017 36th Chinese Control Conf. (CCC)*, Dalian, China, IEEE, 2017, pp. 1441–1446.

[41] K. D. Gupta, A. Rahman, S. Poudyal, M. N. Huda, and M. P. Mahmud, "A hybrid POW-POS implementation against 51 percent attack in cryptocurrency system," in *2019 IEEE Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, IEEE, 2019, pp. 396–403.

[42] X. Yang, Y. Chen, and X. Chen, "Effective scheme against 51% attack on proof-of-work blockchain with history weighted information," in *2019 IEEE Int. Conf. Blockchain (Blockchain)*, IEEE, 2019, pp. 261–265.

[43] S. Lee and S. Kim, "Proof-of-stake at stake: Predatory, destructive attack on PoS cryptocurrencies," in *Proc. 3rd Workshop Cryptocurrencies Blockchains Distrib. Syst.*, 2020, pp. 7–11.

[44] D. Karakostas and A. Kiayias, "Securing proof-of-work ledgers via checkpointing," in *2021 IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, IEEE, 2021, pp. 1–5.

[45] N. Shi, "A new proof-of-work mechanism for bitcoin," *Financ. Innov.*, vol. 2, no. 1, pp. 1–8, 2016. doi: 10.1186/s40854-016-0045-6.

[46] Y. Wang, W. Wu, C. Zhang, X. Xing, X. Gong and W. Zou, "From proof-of-concept to exploitable (one step towards automatic exploitability assessment)," *Cybersecurity*, vol. 2, no. 1, pp. 1–25, 2019. doi: 10.1186/s42400-018-0018-3.

[47] Y. Wu, "Mining threat intelligence from billion-scale SSH brute-force attacks," Doctoral dissertation, Univ. IllinoisUrbana-Champaign: USA, 2020.

[48] A. Abhishta, M. Junger, R. Joosten, and L. J. Nieuwenhuis, "A note on analysing the attacker aims behind DDoS attacks," in *Intelligent Distributed Computing XIII*. Cham: Springer, 2020, vol. 868, pp. 255–265. doi: 10.1007/978-3-030-32258-8_30.

[49] M. Alrizah, S. Zhu, X. Xing, and G. Wang, "Errors, misunderstandings, and attacks: Analyzing the crowdsourcing process of ad-blocking systems," in *Proc. Internet Meas. Conf.*, 2019, pp. 230–244.

[50] N. Rathod and D. Motwani, "Security threats on blockchain and its countermeasures," *Int. Res. J. Eng. Technol.*, vol. 5, no. 11, pp. 1636–1642, 2018.

[51] P. D'Arco, Z. E. Ansaroudi, and F. Mogavero, "Multi-stage proof-of-works: Properties and vulnerabilities," *Theor. Comput. Sci.*, vol. 976, no. 3, 2023, Art. no. 114108. doi: 10.1016/j.tcs.2023.114108.

[52] O. Ajayi and T. Saadawi, "Detecting insider attacks in blockchain networks," in *2021 Int. Symp. Net., Comput. Commun. (ISNCC)*, IEEE, 2021, pp. 1–7.

[53] Y. Jiang and J. Zhang, "Time-restricted double-spending attack on PoW-based blockchains," 2024, *arXiv:2402.17223*.

[54] J. Zheng, H. Huang, Z. Zheng, and S. Guo, "Adaptive double-spending attacks on PoW-based blockchains," *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 3, pp. 1098–1110, 2023.

[55] C. -N. Chou, Y. -J. Lin, R. Chen, H. -Y. Chang, I. -P. Tu and S. -W. Liao, "Personalized difficulty adjustment for countering the double-spending attack in proof-of-work consensus protocols," in *2018 IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Soc. Comput. (CPSCom) IEEE Smart Data (SmartData)*, Halifax, NS, Canada, IEEE, 2018, pp. 1456–1462.

[56] N. A. Akbar, A. Muneer, N. ElHakim, and S. M. Fati, “Distributed hybrid double-spending attack prevention mechanism for proof-of-work and proof-of-stake blockchain consensuses,” *Future Internet*, vol. 13, no. 11, 2021, Art. no. 285. doi: 10.3390/fi13110285.

[57] M. Mirkin, Y. Ji, J. Pang, A. Klages-Mundt, I. Eyal, and A. Juels, “BDoS: Blockchain denial-of-service,” in *Proc. 2020 ACM SIGSAC Conf. Comput. Commun. Secur.*, 2020, pp. 601–619.

[58] Z. Zuo, X. Cao, Y. Wang, and W. Zhang, “Resilient consensus of multiagent systems against denial-of-service attacks,” *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 52, no. 4, pp. 2664–2675, 2021. doi: 10.1109/TSMC.2021.3051730.

[59] D. Zhang and G. Feng, “A new switched system approach to leader-follower consensus of heterogeneous linear multiagent systems with DoS attack,” *IEEE Trans. Syst. Man, Cybern.: Syst.*, vol. 51, no. 2, pp. 1258–1266, 2019. doi: 10.1109/TSMC.2019.2895097.

[60] Z. Feng and G. Hu, “Distributed secure average consensus for linear multi-agent systems under DoS attacks,” in *2017 Am. Control Conf. (ACC)*, IEEE, 2017, pp. 2261–2266.

[61] A. Guru, B. K. Mohanta, H. Mohapatra, F. Al-Turjman, C. Altrjman and A. Yadav, “A survey on consensus protocols and attacks on blockchain technology,” *Appl. Sci.*, vol. 13, no. 4, 2023, Art. no. 2604. doi: 10.3390/app13042604.

[62] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen and E. Dutkiewicz, “Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities,” *IEEE Access*, vol. 7, pp. 85727–85745, 2019. doi: 10.1109/ACCESS.2019.2925010.

[63] S. Fahim, S. K. Rahman, and S. Mahmood, “Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV,” *Int. J. Math. Sci. Comput.*, vol. 3, pp. 46–57, 2023.

[64] H. Poston, “Blockchain security,” in *Coursera Online Course*, Coursera Inc., 2024. Accessed: Jul. 24, 2024. [Online]. Available: https://www.coursera.org/learn/blockchain-security/home/module/1

[65] M. Kaur *et al.*, “Performance analysis of large scale mainstream blockchain consensus protocols,” *IEEE Access*, vol. 9, pp. 80931–80944, 2021.

[66] S. Kanjalkar, J. Kuo, Y. Li, and A. Miller, “Short paper: I can’t believe it’s not stake! resource exhaustion attacks on PoS,” in *Financ. Cryptogr. Data Secur.: 23rd Int. Conf., FC 2019*, Frigate Bay, St. Kitts and Nevis, Springer, 2019, pp. 62–69.

[67] E. Deirmentzoglou, G. Papakyriakopoulos, and C. Patsakis, “A survey on long-range attacks for proof of stake protocols,” *IEEE Access*, vol. 7, pp. 28712–28725, 2019.

[68] O. Sanda, M. Pavlidis, S. Seraj, and N. Polatidis, “Long-range attack detection on permissionless blockchains using deep learning,” *Expert Syst. Appl.*, vol. 218, 2023, Art. no. 119606.

[69] S. Aggarwal and N. Kumar, “Cryptographic consensus mechanisms,” *Adv. Comput.*, vol. 121, pp. 211–226, 2021.

[70] J. -S. Kim, J. -M. Shin, S. -H. Choi, and Y. -H. Choi, “A study on prevention and automatic recovery of blockchain networks against persistent censorship attacks,” *IEEE Access*, vol. 10, pp. 110770–110784, 2022. doi: 10.1109/ACCESS.2022.3214213.

[71] W. Y. M. M. Thin, N. Dong, G. Bai, and J. S. Dong, “Formal analysis of a proof-of-stake blockchain,” in *2018 23rd Int. Conf. Eng. Complex Comput. Syst. (ICECCS)*, IEEE, 2018, pp. 197–200.

[72] M. Platt and P. McBurney, “Sybil attacks on identity-augmented proof-of-stake,” *Comput. Netw.*, vol. 199, 2021, Art. no. 108424. doi: 10.1016/j.comnet.2021.108424.

[73] K. Alachkar and D. Gaastra, “Blockchain-based sybil attack mitigation: A case study of the I2P network,” *August*, vol. 22, pp. 1–13, 2018.

[74] T. Rajab, M. H. Manshaei, M. Dakhilalian, M. Jadliwala, and M. A. Rahman, “On the feasibility of Sybil attacks in shard-based permissionless blockchains,” 2002, *arXiv:2002.06531*.

[75] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong and M. Zhou, “Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism,” *IEEE Access*, vol. 7, pp. 118541–118555, 2019. doi: 10.1109/ACCESS.2019.2935149.

[76] S. M. S. Saad and R. Z. R. M. Radzi, “Comparative review of the blockchain consensus algorithm between proof of stake (POS) and delegated proof of stake (DPOS),” *Int. J. Innov. Comput.*, vol. 10, no. 2, 2020. doi: 10.11113/ijic.v10n2.272.

[77] Y. Yao, F. Tian, and C. Zhang, “The research of an improved blockchain consensus mechanism,” in *2020 2nd Int. Conf. Appl. Mach. Learn. (ICAML)*, IEEE, 2020, pp. 305–310.

[78] C. Zhao, X. Wang, Z. Lu, J. Wang, D. Wang and B. Meng, “HSDVS-DPoS: A secure and heterogeneous DPoS consensus protocol using heterogeneous strong designated verifier signature,” in *Future Inf. Commun. Conf.*, Springer, 2023, pp. 541–562.

[79] M. Larangeira and D. Karakostas, “The security of delegated proof-of-stake wallet and stake pools,” in *Blockchains: A Handbook on Fundamentals, Platforms and Applications*. Cham: Springer, 2023, vol. 105, pp. 225–260. doi: 10.1007/978-3-031-32146-7_8978-3-031-32146-7.

[80] B. Yuan, H. Jin, D. Zou, L. T. Yang, and S. Yu, “A practical byzantine-based approach for faulty switch tolerance in software-defined networks,” *IEEE Trans. Netw. Serv. Manag.*, vol. 15, no. 2, pp. 825–839, 2018. doi: 10.1109/TNSM.2018.2822668.

[81] J. Andrew, D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei and J. Eunice, “Blockchain for healthcare systems: Architecture, security challenges, trends and future directions,” *J. Netw. Comput. Appl.*, vol. 215, 2023, Art. no. 103633. doi: 10.1016/j.jnca.2023.103633.

[82] Y. Meng, Z. Cao, and D. Qu, “A committee-based byzantine consensus protocol for blockchain,” in *2018 IEEE 9th Int. Conf. Softw. Eng. Serv. Sci. (ICSESS)*, IEEE, 2018, pp. 1–6.

[83] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar and K. -K. R. Choo, “HomeChain: A blockchain-based secure mutual authentication system for smart homes,” *IEEE Internet Things J.*, vol. 7, no. 2, pp. 818–829, 2019. doi: 10.1109/JIOT.2019.2944400.

[84] A. Alnuaimi, A. Alshehhi, K. Salah, R. Jayaraman, I. A. Omar and A. Battah, “Blockchain-based processing of health insurance claims for prescription drugs,” *IEEE Access*, vol. 10, pp. 118093–118107, 2022. doi: 10.1109/ACCESS.2022.3219837.

[85] X. Wu, J. Chang, H. Ling, and X. Feng, “Scaling proof-of-authority protocol to improve performance and security,” *Peer Peer Netw. Appl.*, vol. 15, no. 6, pp. 2633–2649, 2022. doi: 10.1007/s12083-022-01371-y.

[86] Y. Hu *et al.*, “A practical heartbeat-based defense scheme against cloning Attacks in PoA blockchain,” *Comput. Stand. Interfaces*, vol. 83, 2023, Art. no. 103656. doi: 10.1016/j.csi.2022.103656.

[87] P. Ekparinya, V. Gramoli, and G. Jourjon, “The attack of the clones against proof-of-authority,” 2019, *arXiv:1902.10244*.

[88] A. Wahab and W. Mehmood, “Survey of consensus protocols,” *arXiv preprint arXiv:1810.03357*, 2018.

[89] R. Chen, Y. Li, Y. Yu, H. Li, X. Chen and W. Susilo, “Blockchain-based dynamic provable data possession for smart cities,” *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4143–4154, 2020. doi: 10.1109/JIOT.2019.2963789.

[90] Y. Wen, F. Lu, Y. Liu, and X. Huang, “Attacks and countermeasures on blockchains: A survey from layering perspective,” *Comput. Netw.*, vol. 191, 2021, Art. no. 107978. doi: 10.1016/j.comnet.2021.107978.

[91] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu and W. Shi, “On security analysis of proof-of-elapsed-time (poet),” in *Stab. Safety Secur. Distrib. Syst.: 19th Int. Symp., SSS 2017*, Boston, MA, USA, Springer, 2017, pp. 282–297.

[92] A. A. Menon, T. Saranya, S. Sureshbabu, and A. Mahesh, “A comparatıve analysis on three consensus algorithms: proof of burn, proof of elapsed time, proof of authority,” in *Computer Networks and Inventive Communication Technologies*. Singapore: Springer 2022, pp. 369–383.

[93] M. Platt and P. McBurney, “Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong Sybil attack resistance,” *Algorithms*, vol. 16, no. 1, 2023, Art. no. 34. doi: 10.3390/a16010034.

[94] T. Krishnamohan, “Proof of identity-a blockchain consensus algorithm to create a dynamically permissioned blockchain,” *Int. J. Blockchains Cryptocurrencies*, vol. 3, no. 4, pp. 289–301, 2022. doi: 10.1504/IJBC.2022.128888.

[95] D. C. Sánchez, “Zero-knowledge proof-of-identity: Sybil-resistant, anonymous authentication on permissionless blockchains and incentive compatible, strictly dominant cryptocurrencies,” 2019, *arXiv:1905.09093*.

[96] H. Lu, J. Li, and M. Guizani, “A novel ID-based authentication framework with adaptive privacy preservation for VANETs,” in *2012 Comput. Commun. Appl. Conf.*, IEEE, 2012, pp. 345–350.

[97] E. Anceaume, A. Pozzo, T. Rieutord, and S. Tucci-Piergiovanni, “On finality in blockchains,” 2012, *arXiv:2012.10172*.

[98] A. Sasikumar, L. Ravi, K. Kotecha, A. Abraham, M. Devarajan and S. Vairavasundaram, “A secure big data storage framework based on blockchain consensus mechanism with flexible finality,” *IEEE Access*, vol. 11, pp. 56712–56725, 2023. doi: 10.1109/ACCESS.2023.32823222169-3536.

[99] S. Garcia-Torres, M. Rey-Garcia, J. Sáenz, and S. Seuring, “Traceability and transparency for sustainable fashion-apparel supply chains,” *J. Fash. Mark. Manag.: Int. J.*, vol. 26, no. 2, pp. 344–364, 2022. doi: 10.1108/JFMM-07-2020-0125.

[100] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, “Privacy-preserving solutions for blockchain: Review and challenges,” *IEEE Access*, vol. 7, pp. 164908–164940, 2019. doi: 10.1109/ACCESS.2019.2950872.

[101] M. Soni and D. K. Singh, “Blockchain implementation for privacy preserving and securing the healthcare data,” in *2021 10th IEEE Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, IEEE, 2021, pp. 729–734.

[102] B. Cao *et al.*, “When Internet of Things meets blockchain: Challenges in distributed consensus,” *IEEE Netw.*, vol. 33, no. 6, pp. 133–139, 2019. doi: 10.1109/MNET.2019.1900002.

[103] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty and Y. Wang, “PoBT: A lightweight consensus algorithm for scalable IoT business blockchain,” *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2343–2355, 2019. doi: 10.1109/JIOT.2019.2958077.

[104] E. Tan, S. Mahula, and J. Crompvoets, “Blockchain governance in the public sector: A conceptual framework for public management,” *Gov. Inf. Q.*, vol. 39, no. 1, 2022, Art. no. 101625. doi: 10.1016/j.giq.2021.101625.

[105] N. Kshetri, “Blockchain technology for improving transparency and citizen’s trust,” *Adv. Inf. Commun.: Proc. 2021 Future Inf. Commun. Conf. (FICC)*, vol. 1, pp. 716–735, 2021. doi: 10.1007/978-3-030-73100-7.

[106] A. Ayub Khan, A. A. Laghari, A. A. Shaikh, S. Bourouis, A. M. Mamlouk and H. Alshazly, “Educational blockchain: A secure degree attestation and verification traceability architecture for higher education commission,” *Appl. Sci.*, vol. 11, no. 22, 2021, Art. no. 10917. doi: 10.3390/app112210917.

[107] S. K. Panda and S. C. Satapathy, “Drug traceability and transparency in medical supply chain using blockchain for easing the process and creating trust between stakeholders and consumers,” *Pers. Ubiquitous Comput.*, pp. 1–17, 2021. doi: 10.1007/s00779-021-01588-3.

[108] A. C. An, P. T. X. Diem, T. Van Toi, and L. D. Q. Binh, “Building a product origins tracking system based on blockchain and PoA consensus protocol,” in *2019 Int. Conf. Adv. Comput. Appl. (ACOMP)*, IEEE, 2019, pp. 27–33.

[109] Y. Xiao, C. Zhou, and Z. Yang, “Improved practical byzantine fault tolerance algorithm based on supply chain,” in *Proc. 2022 6th Int. Conf. Electron. Inf. Technol. Comput. Eng.*, 2022, pp. 1904–1912.

[110] X. Xu, D. Zhu, X. Yang, S. Wang, L. Qi and W. Dou, “Concurrent practical byzantine fault tolerance for integration of blockchain and supply chain,” *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–17, 2021. doi: 10.1145/3395331.

[111] H. Moudoud, S. Cherkaoui, and L. Khoukhi, “An IoT blockchain architecture using oracles and smart contracts: The use-case of a food supply chain,” in *IEEE 30th Annu. Int. Symp. Pers., Indoor Mob. Radio Commun. (PIMRC)*, IEEE, 2019, pp. 1–6.

[112] Z. Auhl, N. Chilamkurti, R. Alhadad, and W. Heyne, “A comparative study of consensus mechanisms in blockchain for IoT networks,” *Electronics*, vol. 11, no. 17, 2022, Art. no. 2694. doi: 10.3390/electronics11172694.

[113] M. Kim and Y. Kim, “Development of IoT device management system using blockchain DPoS consensus algorithm,” *J. IKEEE*, vol. 23, no. 2, pp. 508–516, 2019.

[114] N. Chondros, K. Kokordelis, and M. Roussopoulos, “On the practicality of practical byzantine fault tolerance,” in *Middleware 2012: ACM/IFIP/USENIX 13th Int. Middleware Conf.*, Montreal, QC, Canada, Springer, 2012, vol. 13, pp. 436–455.

[115] L. Li, Y. Chen, and B. Lin, “Intrusion detection analysis of internet of things considering practical byzantine fault tolerance (PBFT) algorithm,” *Wirel. Commun. Mob. Comput.*, vol. 2021, no. 1, pp. 1–9, 2021. doi: 10.1155/2021/6856284.

[116] C. Gonzalez-Amarillo, C. Cardenas-Garcia, M. Mendoza-Moreno, G. Ramirez-Gonzalez, and J. C. Corrales, “Blockchain-IoT sensor (BIoTS): A solution to iot-ecosystems security issues,” *Sensors*, vol. 21, no. 13, 2021, Art. no. 4388. doi: 10.3390/s21134388.

[117] M. M. Yakubu, A. A. Mu’azu, and S. Adamu, “Consensus mechanisms in mitigating privacy concerns within blockchain-based supply chains,” in *17th Int. Istanbul Sci. Res. Congress Life, Eng. Archit. Math. Sci.*, Apr. 2024. doi: 10.5281/zenodo.11093823.

[118] A. A. Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, and S. Kot, “Internet of Things (IoT) security with blockchain technology: A state-of-the-art review,” *IEEE Access*, vol. 10, pp. 122679–122695, 2022. doi: 10.1109/ACCESS.2022.3223370.

[119] C. Wang, J. Shen, and S. Tan, “PoSI: A new consensus protocol based on storage age and data integrity verification,” *J. Int. Technol.*, vol. 22, no. 5, pp. 979–989, 2021. doi: 10.53106/160792642021092205004.

[120] H. Moudoud and S. Cherkaoui, “Multi-tasking federated learning meets blockchain to foster trust and security in the Metaverse,” *Ad Hoc Netw.*, vol. 150, 2023, Art. no. 103264. doi: 10.1016/j.adhoc.2023.103264.

[121] M. Bahrami, A. Movahedian, and A. Deldari, “A comprehensive blockchain-based solution for academic certificates management using smart contracts,” in *2020 10th Int. Conf. Comput. Knowl. Eng. (ICCKE)*, IEEE, 2020, pp. 573–578.

[122] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere, and B. Stiller, “The proposal of a blockchain-based architecture for transparent certificate handling,” in *Business Inf. Syst. Workshops: BIS 2018 Int. Workshops*, Berlin, Germany: Springer, 2019, vol. 21, pp. 185–196.

[123] A. Alam, “Platform utilising blockchain technology for eLearning and online education for open sharing of academic proficiency and progress records,” in *Smart Data Intell.: Proc. ICSMDI 2022*, Springer, 2022, pp. 307–320.

[124] S. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz and W. Knottenbelt, “SoK: Decentralized finance (DeFi),” in *Proc. 4th ACM Conf. Adv. Finan. Technol.*, 2022, pp. 30–46.

[125] D. Stamatakis, D. G. Kogias, P. Papadopoulos, P. A. Karkazis, and H. C. Leligou, “Blockchain-powered gaming: Bridging entertainment with serious game objectives,” *Computers*, vol. 13, no. 1, 2024, Art. no. 14. doi: 10.3390/computers13010014.

[126] S. Onopa and Z. Kotulski, “State-of-the-art and New challenges in 5G networks with Blockchain Technology,” *Electronics*, vol. 13, no. 5, 2024, Art. no. 974. doi: 10.3390/electronics13050974.

[127] P. Prabha and K. Chatterjee, “Design and implementation of hybrid consensus mechanism for IoT based healthcare system security,” *Int. J. Inf. Tecnol.*, vol. 14, no. 3, pp. 1381–1396, 2022. doi: 10.1007/s41870-022-00880-6.

[128] S. Ghosh and R. S. Dutta, “A hybrid blockchain consensus algorithm using locational marginal pricing for energy applications,” in *2021 IEEE Int. IOT, Electron. Mechatron. Conf. (IEMTRONICS)*, IEEE, 2021, pp. 1–8.

[129] J. -T. Kim, J. Jin, and K. Kim, “A study on an energy-effective and secure consensus algorithm for private blockchain systems (PoM: Proof of Majority),” in *2018 Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, IEEE, 2018, pp. 932–935.

[130] K. Košťál, T. Krupa, M. Gembec, I. Vereš, M. Ries and I. Kotuliak, “On transition between PoW and PoS,” in *2018 Int. Symp. ELMAR*, IEEE, 2018, pp. 207–210.

[131] J. Li, D. Han, Z. Wu, J. Wang, K. -C. Li and A. Castiglione, “A novel system for medical equipment supply chain traceability based on alliance chain and attribute and role access control,” *Future Gener. Comput. Syst.*, vol. 142, no. 2, pp. 195–211, 2023. doi: 10.1016/j.future.2022.12.037.

[132] T. M. Fernandez-Carames and P. Fraga-Lamas, “Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks,” *IEEE Access*, vol. 8, pp. 21091–21116, 2020. doi: 10.1109/ACCESS.2020.2968985.

[133] M. Allende *et al.*, “Quantum-resistance in blockchain networks,” *Sci. Rep.*, vol. 13, no. 1, 2023, Art. no. 5664. doi: 10.1038/s41598-023-32701-6.

[134] J. J. Kearney and C. A. Perez-Delgado, “Vulnerability of blockchain technologies to quantum attacks,” *Array*, vol. 10, 2021, Art. no. 100065. doi: 10.1016/j.array.2021.100065.

[135] O. Grote, A. Ahrens, and C. Benavente-Peces, “A review of post-quantum cryptography and crypto-agility strategies,” in *2019 Int. Interdiscip. PhD Workshop (IIPhDW)*, IEEE, 2019, pp. 115–120.

[136] W. Cui, T. Dou, and S. Yan, “Threats and opportunities: Blockchain meets quantum computation,” in *2020 39th Chinese Control Conf. (CCC)*, IEEE, 2020, pp. 5822–5824.

[137] J. Gomes, S. Khan, and D. Svetinovic, “Fortifying the blockchain: A systematic review and classification of post-quantum consensus solutions for enhanced security and resilience,” *IEEE Access*, vol. 11, pp. 74088–74100, 2023. doi: 10.1109/ACCESS.2023.3296559.

[138] G. Kondova and R. Barba, “Governance of decentralized autonomous organizations,” *J. Mod. Account Audit.*, vol. 15, no. 8, pp. 406–411, 2019. doi: 10.17265/1548-6583/2019.08.003.

[139] C. Tozzi, “Decentralizing democracy: Approaches to consensus within blockchain communities,” *Teknokultura: Revista De Cultura Digital Y Movimientos Sociales*, vol. 16, no. 2, pp. 181–195, 2019. doi: 10.5209/tekn.64523.

[140] A. Zwitter and J. Hazenberg, “Decentralized network governance: Blockchain technology and the future of regulation,” *Front. Blockchain*, vol. 3, 2020, Art. no. 12. doi: 10.3389/fbloc.2020.00012.

[141] P. Centobelli, R. Cerchione, P. D. Vecchio, E. Oropallo, and G. Secundo, “Blockchain technology for bridging trust, traceability and transparency in circular supply chain,” *Inf. Manag.*, vol. 59, no. 7, 2022, Art. no. 103508. doi: 10.1016/j.im.2021.103508.

[142] M. Ruan, H. Gao, and Y. Wang, “Secure and privacy-preserving consensus,” *IEEE Trans. Automat. Contr.*, vol. 64, no. 10, pp. 4035–4049, 2019. doi: 10.1109/TAC.2019.2890887.

[143] M. Tan, G. Xu, J. Yang, and L. Ding, “Blockchain privacy consensus mechanism based on threshold signature,” in *2021 3rd Int. Acad. Exch. Conf. Sci. Technol. Innov. (IAECST)*, IEEE, 2021, pp. 582–585.

[144] T. T. Ramanathan, “Survey on consensus algorithms in blockchain for secure data sharing,” *I-Manag. J. Cloud Comput.*, vol. 7, no. 1, pp. 26–31. doi: 10.26634/jcc.7.1.17114.

[145] B. Sowmiya and E. Poovammal, “Methods and techniques for privacy preserving in blockchain,” in *2020 3rd Int. Conf. Intell. Sustain. Syst. (ICISS)*, IEEE, 2020, pp. 1346–1351.

[146] J. Sunny, N. Undralla, and V. M. Pillai, “Supply chain transparency through blockchain-based traceability: An overview with demonstration,” *Comput. Indust. Eng.*, vol. 150, 2020, Art. no. 106895. doi: 10.1016/j.cie.2020.106895.

[147] A. A. Khan *et al.*, “Blockchain-enabled infrastructural security solution for serverless consortium fog and edge computing,” *PeerJ Comput. Sci.*, vol. 10, pp. 1–34, 2024. doi: 10.7717/peerj-cs.1933.

[148] M. Saad, Z. Qin, K. Ren, D. Nyang, and D. Mohaisen, “e-PoS: Making proof-of-stake decentralized and fair,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 8, pp. 1961–1973, 2021. doi: 10.1109/TPDS.2020.3048853.

[149] P. Tasca, J. Xu, N. Vadgama, and J. I. Ibañez, “Energy footprint of blockchain consensus mechanisms beyond proof-of-work,” 2021, *arXiv:2109.03667*.

[150] W. Bouzegag, L. Belaiche, L. Kahloul, and H. Bennoui, “Leveraging formal methods to blockchain consensus protocols: A scoping literature review,” in *2022 Int. Sym. iNnovative Inf. Biskra (ISNIB)*, IEEE, 2022, pp. 1–6.

[151] H. Afzaal, M. Imran, M. U. Janjua, and S. P. Gochhayat, “Formal modeling and verification of a blockchain-based crowdsourcing consensus protocol,” *IEEE Access*, vol. 10, pp. 8163–8183, 2022. doi: 10.1109/ACCESS.2022.3141982.