OPUS-HSO

Repositorium der Hochschule Offenburg
https://opus.hs-offenburg.de

Hybrid Consensus Mechanisms in Blockchain: A Comprehensive Review

Ali Ahmed Al-awamy, Nagi Ali Al-shaibany, Axel Sikora, Dominik Welte

Zitiervorschlag im APA Stil:

Al-awamy, A. A., Al-shaibany, N. A., Sikora, A., & Welte, D. (2025). Hybrid Consensus Mechanisms in Blockchain: A Comprehensive Review. *International Journal of Intelligent Systems*, *2025*(1), 1–31. https://doi.org/10.1155/int/5821997

Abstract

Blockchain technology, renowned for its foundational attributes of decentralization, security, and immutability, offers substantial potential for diverse applications. At the heart of blockchain functionality are consensus mechanisms, crucial for preserving the decentralized integrity of the network. However, traditional consensus algorithms like Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT) typically require significant computational and communication resources, which may not be feasible for resource-limited environments. The purpose of this paper is to explore hybrid consensus algorithms that integrate conventional consensus mechanisms with advanced nonlinear data structures. We comprehensively analyze a wide range of hybrid consensus mechanisms, emphasizing their architectural design, operational efficiencies, and ability to address both consensus-specific vulnerabilities and network-level threats, such as Sybil attacks, double-spending, and partitioning attacks. To achieve this, we employ a set of comprehensive evaluation criteria for blockchain technologies, namely, validation, IoT, real-time processing, application suitability, security, and implementation. These criteria help assess the adaptability and efficacy of each mechanism in diverse operational contexts. Through this examination, the paper seeks to illuminate the significant contributions and implications of hybrid consensus mechanisms, guiding stakeholders, researchers, and developers toward making informed decisions about optimizing blockchain technology for their specific needs and inspiring the development of innovative solutions.

Nutzungsbedingungen

Dieses Dokument wird unter diesen Bedingungen zur Verfügung gestellt:
Creative Commons - CC BY - Namensnennung 4.0 International
Für weitere Informationen siehe:
https://creativecommons.org/licenses/by/4.0/deed.de

Kontakt

Hochschule Offenburg | Bibliothek
Badstraße 24
77652 Offenburg
Telefon: (0781) 205-240
E-Mail: bibliothek@hs-offenburg.de
www.hs-offenburg.de/bibliothek

Check for updates

Wiley
International Journal of Intelligent Systems
Volume 2025, Article ID 5821997, 31 pages
https://doi.org/10.1155/int/5821997

WILEY

Review Article

Hybrid Consensus Mechanisms in Blockchain: A Comprehensive Review

Ali Ahmed Al-awamy[1], **Nagi Al-shaibany**[1], **Axel Sikora**[2] **and Dominik Welte**[3]

[1]*Department of Computer and Information Technology, Sana'a University, Sana'a, Yemen*
[2]*Institute for Reliable Embedded Systems and Communication Electronics (ivESK) Offenburg University Badstrasse 24, Offenburg D77652, Germany*
[3]*Department of Embedded Systems and Communication Electronics, Offenburg University, Offenburg, Baden-Württemberg 77652, Germany*

Correspondence should be addressed to Ali Ahmed Al-awamy; ali.al-awamy@su.edu.ye

Received 4 July 2024; Accepted 10 April 2025

Academic Editor: Stefano Cirillo

Copyright © 2025 Ali Ahmed Al-awamy et al. International Journal of Intelligent Systems published by John Wiley & Sons Ltd. This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

Blockchain technology, renowned for its foundational attributes of decentralization, security, and immutability, offers substantial potential for diverse applications. At the heart of blockchain functionality are consensus mechanisms, crucial for preserving the decentralized integrity of the network. However, traditional consensus algorithms like Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT) typically require significant computational and communication resources, which may not be feasible for resource-limited environments. The purpose of this paper is to explore hybrid consensus algorithms that integrate conventional consensus mechanisms with advanced nonlinear data structures. We comprehensively analyze a wide range of hybrid consensus mechanisms, emphasizing their architectural design, operational efficiencies, and ability to address both consensus-specific vulnerabilities and network-level threats, such as Sybil attacks, double-spending, and partitioning attacks. To achieve this, we employ a set of comprehensive evaluation criteria for blockchain technologies, namely, validation, IoT, real-time processing, application suitability, security, and implementation. These criteria help assess the adaptability and efficacy of each mechanism in diverse operational contexts. Through this examination, the paper seeks to illuminate the significant contributions and implications of hybrid consensus mechanisms, guiding stakeholders, researchers, and developers toward making informed decisions about optimizing blockchain technology for their specific needs and inspiring the development of innovative solutions.

Keywords: application suitability; blockchain; hybrid consensus; implementation; IoT; real-time processing; security; validation

1. Introduction

Blockchain technology, initially pioneered by Bitcoin, has rapidly evolved from its cryptographic roots to become a foundational technology across a multitude of industries. Blockchain technology, recognized for its decentralization, immutability, and security, has revolutionized industries such as finance, healthcare, and supply chain management. However, its core component—the consensus mechanism—faces critical challenges.

Traditional consensus mechanisms, such as Proof of Work (PoW) and Proof of Stake (PoS), have proven effective but come with limitations. For instance, PoW offers robust security but is highly energy-intensive [1, 2], while PoS improves efficiency but raises questions about decentralization and fairness [3]. To address these limitations, hybrid consensus mechanisms have emerged as innovative solutions. By combining the strengths of multiple consensus protocols, hybrid mechanisms aim to enhance security, scalability, and energy efficiency. For example, integrating PoW's security with PoS's energy efficiency results in blockchain systems capable of achieving faster transaction validation and lower energy consumption. These benefits make hybrid models particularly attractive for emerging

applications such as the Internet of Things (IoT), where resource constraints demand scalable and lightweight solutions. Despite the growing interest in hybrid consensus models, a comprehensive review of their design, application, and performance remains scarce.

Several studies have reviewed traditional consensus mechanisms and their applications. For example, Bouraga provided a taxonomy of PoW and PoS protocols but omitted hybrid models and third-generation approaches [4]. Similarly, works by Elgountery et al. [5] and Guru et al. [6, 7] explored consensus mechanisms for IoT, while other studies [8, 9] lacked comparative analyses of hybrid approaches. Bodkhe et al. discussed IoT–blockchain integration, focusing primarily on directed acyclic graph (DAG) protocols and not addressing how hybrid mechanisms could optimize performance [10]. Despite these valuable contributions, several important studies have identified critical challenges in consensus mechanisms. For example, Saad et al. [1, 11] provided empirical comparisons and evaluations of consensus algorithms but do not comprehensively examine hybrid mechanisms. Similarly, Heo et al. [2] and Tran et al. [12] focus on network vulnerabilities in blockchain systems but omit discussions on hybrid approaches. Saad et al. [1] highlighted blockchain security challenges, including double-spending and partition attacks, but do not explore hybrid models as a potential solution.

While existing studies provide valuable insights into traditional consensus mechanisms, a systematic evaluation of hybrid consensus mechanisms, particularly their adaptability to IoT environments, remains underexplored. This paper bridges the existing research gap by providing a comprehensive review of hybrid consensus mechanisms with a focus on their performance, adaptability, and security in emerging blockchain applications, particularly for IoT environments and real-time processing. By systematically analyzing six critical aspects—validation, IoT, real-time processing, application suitability, security, and implementation—we highlight how hybrid models address the limitations of traditional approaches and meet the unique challenges of resource-constrained systems.

1. Validation: Hybrid mechanisms enhance transaction and block verification by leveraging the complementary strengths of different protocols. For instance, combining PoW's security with PoS's efficiency improves fraud protection and accelerates data validation, making hybrid systems suitable for applications requiring high security, such as financial transactions or blockchain-based voting systems.
2. IoT: In IoT applications, where devices are constrained by limited computational power and connectivity, hybrid consensus mechanisms provide scalable and resource-efficient solutions. They are designed to adapt to the unique requirements of IoT environments, ensuring effective and secure blockchain integration despite low-power hardware.
3. Real-Time Processing: Hybrid approaches facilitate near-instantaneous consensus, enabling real-time data validation critical for latency-sensitive applications. Examples include autonomous vehicles, supply chain monitoring, and healthcare systems, where delays in processing could result in severe consequences.
4. Application Suitability: Different hybrid models are tailored to specific environments. For example, Casper balances security and energy efficiency, while Microchain and Hybrid Delegated Proof of Authority excel in IoT applications, where cost-effectiveness and resource optimization are paramount.
5. Security: Hybrid mechanisms significantly bolster blockchain security by addressing common vulnerabilities. Systems like Microchain utilize advanced cryptographic methods to mitigate double-spending and long-range attacks, while solutions like Hedera and Hybrid Delegated Proof of Authority defend against Sybil attacks, selfish mining, and other threats through multilayered validation processes.
6. Implementation: While implementing hybrid mechanisms poses challenges such as complexity, synchronization, and resource constraints, strategies like edge computing and optimized communication protocols enable efficient scaling without compromising decentralization or security. Real-world examples, such as Microchain's deployment on Raspberry Pi devices, demonstrate the practical benefits and versatility of hybrid consensus systems.

Through a detailed comparison of various hybrid consensus models, this study critically examines their efficiencies, strengths, and limitations. By addressing key performance metrics such as transaction throughput, latency, and scalability, we provide insights into the adaptability of hybrid mechanisms for applications requiring high security, real-time processing, and resource efficiency. This review also identifies how hybrid consensus mechanisms overcome challenges in blockchain systems, particularly for resource-limited environments, and highlights opportunities for further optimization. By providing a clear roadmap for future research and implementation, this work advances the design of scalable, secure, and efficient blockchain solutions.

1.1. Paper Organization. This survey provides a comprehensive overview of hybrid consensus mechanisms within blockchain technology.

- Section 2: Consensus Mechanisms Overview—This section begins with a discussion of traditional consensus mechanisms, such as PoW and PoS, highlighting their roles and limitations in blockchain environments. These limitations underscore the need for hybrid approaches. Additionally, the section reviews key studies on consensus algorithms to contextualize our research within the broader academic discourse. The related work is summarized in Table 1,

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Table 1: Comparative analysis of review papers on consensus algorithms.

Ref	Year	Contribution	Type of survey	Latency	Throughput	DAG	IoT adaptability	Real time	Application use case	Hybrid consensus
[13]	2022	Development of an ontology for consensus algorithms. Classification and analysis of various consensus algorithms	Comprehensive	✓	✓	✓	✓	N/A	✓	N/A
[4]	2021	Classification framework for blockchain consensus protocols. Highlights differences between protocols	Comprehensive	✓	✓	✓	✓	N/A	✓	N/A
[14]	2020	Comparative and analytical review of blockchain consensus algorithms. Performance evaluation criteria	Comparative and analytical	N/A	✓	✓	✓	N/A	✓	N/A
[15]	2020	Review of blockchain for IoT networks. Consensus methods and implementations	Comprehensive	✓	✓	✓	✓	N/A	N/A	N/A
[5]	2023	Comparative study of BCoT architectures. Proposed IoT architecture	Comparative	N/A	N/A	N/A	✓	N/A	N/A	N/A
[6]	2023	Cryptocurrency technical specifications. Bitcoin as a new payment system	Informative	✓	N/A	N/A	✓	N/A	✓	N/A
[16]	2018	Blockchain consensus for IoT networks. Reducing computational power and convergence time	Overview	✓	✓	✓	✓	N/A	✓	N/A
[10]	2020	Decentralized consensus for CPS applications. Networking and security solutions	Comprehensive	✓	✓	✓	✓	✓	✓	N/A
[17]	2020	Analysis of consensus algorithms. Decision tree tool for testing algorithms	Comprehensive	✓	✓	✓	N/A	N/A	N/A	N/A
[8]	2022	Systematic review of hybrid blockchains. Motivations, technologies, challenges	Systematic	✓	✓	N/A	✓	N/A	✓	N/A
[18]	2018	Blockchain solves centralized ledger issues. Consensus algorithms for agreement	Overview	✓	N/A	N/A	N/A	N/A	N/A	N/A
[19]	2023	Overview of blockchain technology. Security issues and cryptography	Overview	N/A	✓	N/A	✓	N/A	✓	N/A
[7]	2023	IoT security using blockchain and privacy preservation	Comprehensive	✓	✓	N/A	✓	N/A	✓	N/A
[20]	2023	Analysis of blockchain applications in IoT, cloud, social media	Systematic	✓	✓	✓	✓	✓	✓	✓
[21]	2024	Blockchain integration in IoT. Technology, security, scalability, data integrity	Comprehensive	✓	✓	✓	✓	✓	✓	N/A
[22]	2023	Comprehensive analysis of blockchain technology, its challenges, consensus algorithms, and application areas. Unique discussion of situations where blockchain should be avoided	Comprehensive	✓	✓	✓	N/A	N/A	✓	N/A
[23]	2020	Systematic analysis of blockchain consensus algorithms, highlighting performance and security trade-offs	Comprehensive	✓	✓	N/A	✓	✓	✓	N/A
[24]	2020	Focus on consensus mechanisms in private blockchain systems, discussing security, efficiency, and scalability	Informative	✓	✓	N/A	N/A	N/A	✓	N/A
[25]	2022	Comprehensive review of blockchain consensus algorithms, with insights into their technical and operational aspects	Comprehensive	✓	✓	N/A	✓	N/A	N/A	N/A
[26]	2022	Analysis of consensus mechanisms in public blockchains for cryptocurrencies	Comparative	✓	✓	N/A	N/A	N/A	✓	N/A
[27]	2021	Discussion of consensus mechanisms, focusing on their applications, limitations, and future directions	Overview	✓	N/A	N/A	N/A	N/A	✓	N/A

Abbreviations: BCoT, Blockchain of Things; DAG, directed acyclic graph; IoT adaptability, Internet of Things adaptability; N/A, not applicable.

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/5821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

which highlights pivotal studies and their contributions to the field.

- Section 3: Development of Hybrid Consensus Mechanisms—Foundational concepts of hybrid consensus mechanisms are introduced and compared with traditional models. This section also classifies hybrid mechanisms based on six critical aspects: validation, IoT compatibility, real-time processing, application suitability, security, and implementation, offering a detailed understanding of their design and operational nuances.
- Section 4: Analysis of Hybrid Consensus Mechanisms—This section provides an in-depth analysis of significant research works that utilize hybrid consensus models. The analysis categorizes these mechanisms into six key areas—validation, IoT, real-time processing, application suitability, security, and implementation—to demonstrate how hybrid approaches address diverse requirements across blockchain applications.
- Section 5: Conclusion and Future Directions—The paper concludes with a synthesis of findings, summarizing the key contributions of hybrid consensus mechanisms and their broader implications for blockchain technology. Additionally, this section highlights future research opportunities, providing a roadmap for advancing scalability, security, and efficiency in blockchain systems.

This structured approach ensures a systematic and thorough examination of hybrid consensus mechanisms while addressing critical challenges and gaps in the existing literature.

2. Consensus Mechanisms in Blockchain

Consensus is a foundational concept in blockchain technology, ensuring agreement on the state of the distributed ledger across a decentralized network. It plays a critical role in validating transactions, maintaining data integrity, and upholding the security and reliability of the system [28].

Traditional consensus mechanisms, such as PoW and PoS, have been pivotal in blockchain's development. PoW relies on computational effort to validate transactions, while PoS uses stake-based validation to achieve consensus. Despite their effectiveness, these mechanisms face significant challenges, including scalability, energy inefficiency, and limitations in adapting to resource-constrained environments like the IoT [29, 30].

To address these challenges, hybrid consensus mechanisms have emerged as innovative solutions, combining features of traditional models to enhance performance, security, and adaptability. This paper provides a systematic review of hybrid consensus mechanisms, focusing on their application in IoT and real-time processing scenarios. By evaluating key aspects such as validation, IoT suitability, real-time processing, security, and implementation, we highlight how hybrid models overcome the limitations of traditional approaches and meet the demands of emerging blockchain applications.

2.1. Traditional Consensus Mechanisms. Consensus mechanisms are fundamental protocols in blockchain technology, ensuring that all nodes in a decentralized network reach agreement on the state of the ledger. These mechanisms validate transactions, maintain security, and safeguard network integrity by requiring consensus across all participants in the network [18].

Different consensus algorithms have distinct advantages and drawbacks, each offering unique trade-offs in terms of security, scalability, efficiency, and decentralization. For instance, PoW, widely used in systems like Bitcoin, is highly secure but requires vast computational resources, leading to significant energy consumption. PoS, on the other hand, provides better energy efficiency but raises concerns about network centralization, as participants with larger stakes exert greater influence [9].

Other algorithms aim to address these challenges as follows:

- Delegated Proof of Stake (DPoS): Improves transaction throughput by delegating validation to a select group of nodes.
- Practical Byzantine Fault Tolerance (PBFT): Enhances fault tolerance in permissioned networks.
- Proof of Burn (PoB): Incentivizes long-term commitment by burning coins to increase mining chances in future cycles.
- Proof of Reputation (PoR): Ensures fast and energy-efficient consensus using reliable registers.
- Proof of Authority (PoA): Leverages the identity and reputation of validators to achieve faster transactions and lower computational requirements.

These algorithms are further summarized in Table 2, which provides a comparative overview of their primary benefits and limitations. It sheds light on why certain consensus models are integrated into hybrid mechanisms. By combining the strengths of various models, hybrid consensus mechanisms aim to overcome the limitations of individual algorithms, optimizing performance and security across blockchain networks.

These traditional consensus algorithms, while effective, often face challenges in specific blockchain environments. Issues such as limited scalability, high energy consumption, and susceptibility to attacks hinder their suitability for all applications.

Hybrid consensus mechanisms address these challenges by combining the strengths of multiple algorithms. For example, integrating PoW with PoS reduces energy consumption while maintaining robust security. Similarly, DPoS is well-suited for resource-constrained environments, such as the IoT, as it achieves high scalability and efficiency by delegating transaction validation to a select group of nodes, thereby reducing computational overhead.

By adopting hybrid approaches, blockchain networks can achieve improved scalability, security, energy efficiency, and decentralization. These adaptable solutions cater to the diverse requirements of modern blockchain applications,

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Table 2: Assessment of different consensus algorithms.

S.N	Name	Ref	Advantage	Disadvantage
1	PoW	[16]	Nodes having high computation power will be selected as miner	It suffers from 51% attack
2	PoS	[31]	Nodes having lots of money will be selected as miner	Miners have to gather 10% coins of blockchain network
3	DPoS	[32]	Nodes having huge number of votes by delegates will be selected as miner	Probability of getting selected as miner increases if delegates are convinced for votes by incentives like currencies, gadgets, etc.
4	PBFT	[19]	Block created by different clients is instantly finalized in the blockchain network	It suffers from Sybil attack
5	PoB	[33]	Nodes burn more coins so chances of being a miner in later cycles increase	Miner risks a loss of position if the value of the exchanged digital currency suddenly decreases
6	PoXR	[13]	Reward or punishment module is implemented based on behavior during deployment	Huge number of parameters are required to implement reward or punishment module
7	PoR	[34]	Very fast, scalable, and energy-efficient; reliable registers for quick bootstrap; encrypted communication channels	Reliable registers for quick bootstrap. Encrypted communication channels
8	PoA	[35]	Validators are selected based on their identity and reputation, leading to faster transactions and lower computational requirements	Centralization risk due to reliance on a limited number of trusted validators

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/5821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

enabling their deployment in scenarios that demand high performance and resilience.

2.2. Related Work. The development of consensus algorithms has been extensively documented in the literature, emphasizing their evolution and application across various blockchain environments. This paper reviews several pivotal studies to contextualize our research within the broader academic discourse, as summarized in Table 1.

Bouraga's [4] taxonomy traces the evolution of consensus algorithms, from PoW to PoS, categorizing them based on origin, design, performance, and security. However, it mainly addresses general blockchain applications and does not discuss third-generation consensus algorithms or their specific use in IoT environments.

Another notable study by Salimitari and Chatterjee [16] provides a comprehensive analysis of consensus methods tailored for blockchain systems in resource-constrained IoT networks. Their work focuses on addressing key challenges specific to IoT environments, including limited computational power, intermittent network connectivity, and the need for energy-efficient solutions. The study explores various consensus algorithms, including PoW, PoS, PBFT, and DAGs, evaluating their suitability based on factors like computational requirements, energy efficiency, scalability, and fault tolerance. The paper also discusses optimization techniques and security considerations specific to IoT networks. The conclusion emphasizes the need for further research to develop efficient and secure consensus mechanisms tailored for resource-constrained IoT environments.

Elgountery et al. [5] focused on the application of consensus algorithms within resource-constrained IoT networks. It offers an extensive assessment of both traditional and third-generation methods, considering factors such as latency and throughput, and incorporates discussions on DAG consensus models. However, this study lacked a comparative analysis of these methods, particularly in terms of adaptability for IoT applications.

Guru et al. [6] evaluated consensus mechanisms suitable for both legacy and nonlinear algorithms but failed to extend their focus to resource-constrained IoT systems, which are critical for the practical deployment of blockchain technologies in such environments.

Bodkhe et al. [10] examined the intersection of IoT and blockchain, discussing not only the architectural and application aspects of IoT but also including examples of IoT applications that utilize DAG protocols. In contrast, Khobragade and Turuk [17] provide a comprehensive review of blockchain-based IoT, emphasizing security, robustness, and self-maintenance, thereby illustrating how blockchain technology could transform cloud-centered IoT environments.

Tripathi et al. [22] provided critical insights into cases where blockchain technology may not be suitable. They highlight several limitations, including performance challenges in applications requiring high throughput and low latency, such as real-time systems. Additionally, blockchain is less efficient in centralized environments with established trust, where traditional databases are more cost-effective. Resource constraints are another significant issue, as lightweight systems like IoT devices with limited power and storage struggle to meet blockchain's resource demands. Environmental concerns also complicate its adoption, with energy-intensive consensus mechanisms like PoW being impractical for low-value or environmentally sensitive applications. Lastly, blockchain's immutability, while a strength in many contexts, becomes a drawback for use cases requiring frequent data updates or deletions. The authors conclude by emphasizing the need for a careful evaluation of application requirements and suggest exploring alternative or hybrid approaches to address blockchain's inherent limitations.

Recent works, such as Alsunaidi and Alhaidari [25] and Ferdous et al. [23], delve into hybrid consensus mechanisms and their applications in IoT environments. Alsunaidi and Alhaidari [25] provide a comprehensive review of consensus algorithms, with particular emphasis on their technical and operational aspects. They evaluate the adaptability of hybrid mechanisms to IoT networks, focusing on their ability to address resource constraints and maintain energy efficiency. The study also discusses the integration of DAGs as a potential solution for improving scalability and reducing latency in IoT-specific use cases.

Ferdous et al. [23] systematically analyzed blockchain consensus mechanisms, highlighting trade-offs between performance, security, and scalability. Their work examines various consensus protocols, such as PoW, PoS, and PBFT, in the context of hybrid designs. The authors emphasize the importance of balancing computational efficiency with network decentralization, particularly in IoT environments where devices are resource-constrained. Additionally, the study outlines future directions for developing lightweight consensus mechanisms capable of meeting the demands of real-time applications.

These studies underscore the critical need for further research into hybrid consensus mechanisms that can address performance and scalability challenges in IoT and other resource-constrained environments. By exploring the integration of existing algorithms with novel approaches, these works lay the groundwork for more efficient and adaptable blockchain solutions.

This study underscores the importance of recognizing blockchain's limitations and conducting a thorough evaluation of application requirements. The authors advocate for exploring alternative or hybrid approaches in cases where the drawbacks of blockchain outweigh its benefits, ensuring more suitable and efficient solutions for diverse use cases.

While these contributions are valuable, they often overlook detailed comparisons of third-generation consensus methods or the applicability of DAG systems for IoT-specific challenges. It is also observed that current literature tends to rely on intuitive categorization of domain knowledge, which might obscure the inherent logical connections between concepts within the field.

Table 1 provides a comparative analysis of various review papers on consensus algorithms within blockchain technology, with the objective of shedding light on the current landscape of literature in this crucial domain. The selection

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

of these papers was meticulously curated to encompass a diverse range of contributions, survey methodologies, and coverage areas, allowing for a comprehensive exploration of the nuances and gaps within the existing literature.

Through this analysis, our aim is to identify and elucidate the gaps in the literature, particularly in the exploration of hybrid consensus mechanisms. The table categorizes these papers based on several key aspects, including their contribution to the field, the type of survey conducted, the tools used in the analysis, and the coverage of consensus algorithms.

The analysis of consensus algorithms in blockchain technology, as outlined in Table 1, highlights the diverse approaches taken by various review studies, providing a clearer understanding of how these studies interpret and discuss the development of consensus mechanisms in different blockchain environments. Some reviews focus on traditional consensus algorithms, primarily emphasizing cryptographic principles, while others delve into the complexities of hybrid blockchains that integrate both public and private architecture elements. Despite these valuable contributions, a significant gap remains in the literature, particularly regarding the application of hybrid consensus mechanisms tailored for specialized use cases like the IoT.

Several studies, such as those by Alkhateeb et al. [8], examine the platforms commonly utilized to integrate blockchain with IoT. These studies highlight platforms like Ethereum, known for its robust smart contract capabilities, alongside other blockchain networks such as EOS, Bitcoin, Litecoin, and Ripple. These platforms are primarily discussed in terms of storing IoT data, facilitating private communications, and supporting decentralized applications. However, most reviews focus on the general applications of these platforms, rather than investigating how hybrid consensus mechanisms can optimize these platforms for improved IoT performance. This represents a key underexplored area in the literature.

Our study fills this gap by providing the first comprehensive evaluation of hybrid consensus algorithms specifically in the context of IoT, a critical area where existing literature tends to focus on traditional consensus models or generalized blockchain applications. This contribution is significant in shifting the focus from a generalized view of blockchain platforms to a more detailed exploration of how hybrid consensus mechanisms can provide tailored solutions for IoT integration.

Incorporating insights from recent works, including Bouraga's [4] taxonomy and Gedam and Karmore's review [21], we explore how the evolution of consensus algorithms—from PoW to PoS and beyond—has paved the way for more scalable and efficient blockchain architectures. Bouraga's taxonomy traces this evolution, while Gedam and Karmore's comprehensive review on blockchain–IoT integration emphasizes challenges around security and scalability. Both studies reinforce the importance of addressing scalability and security in IoT environments, where blockchain plays a crucial role in ensuring data integrity and providing secure, scalable solutions. Our study is innovative in its exclusive focus on hybrid consensus mechanisms, exploring how they uniquely contribute to improving IoT integration. By offering a deeper understanding of how these mechanisms function in real-world IoT applications, we provide valuable insights into deploying more efficient and scalable blockchain solutions in an increasingly interconnected world.

3. Hybrid Consensus Mechanisms

Hybrid consensus mechanisms try to optimize blockchain functionality by combining multiple consensus algorithms within a single network. This approach aims to leverage the strengths and mitigate the weaknesses of each mechanism to enhance overall system performance. The design of hybrid consensus mechanisms involves detailed planning to ensure seamless interoperability among various algorithms. It is essential to uphold robust security measures and effectively address potential conflicts or vulnerabilities that may arise from the integration of different systems [14].

3.1. Examples of Hybrid Consensus Mechanisms in Blockchain

3.1.1. PoW and PoS Hybrids. In an effort to optimize blockchain technology for both security and energy efficiency, some networks employ a hybrid consensus mechanism that combines PoW and PoS. This approach allows for the strengths of one mechanism to complement the weaknesses of the other, effectively balancing the need for energy-intensive block creation with a more energy-efficient process for transaction validation within those blocks [36].

3.1.1.1. Operational Dynamics

- Block Creation: Utilizes PoW, where miners solve complex computational problems to create new blocks. This process, while energy-intensive, is renowned for its high security and difficulty in being compromised.
- Transaction Validation: Employs PoS for the subsequent validation of transactions within these blocks. In PoS, validators are chosen based on the number of coins they hold and are willing to *stake* as collateral, which consumes significantly less energy compared to PoW.

3.1.1.2. Example: Casper Blockchain. The Casper Blockchain exemplifies this hybrid approach by integrating PoS with the traditional Ethash algorithm of PoW. Casper enhances the economic and security aspects of the consensus mechanism through a novel stake-based validation protocol.

3.1.1.3. Casper's Stake-Based Consensus System

- Security Deposits: Validators on the Casper network must deposit a security amount to participate in the consensus process. This deposit acts both as a gatekeeper mechanism to ensure that only serious validators participate and as a punitive measure to deter dishonesty [37].

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

- Reward and Risk Mechanism: Validators stand to gain rewards based on transaction fees and the number of transactions they help validate. However, producing an *invalid* block can result in the loss of their deposits and exclusion from the consensus network.
- Betting System Analogy: The PoS component of Casper can be likened to a betting system, where validators *bet* on blocks they believe are valid. Successful validators who bet on the right blocks receive monetary rewards, aligning individual incentives with network security.

3.1.1.4. Security Enhancements. Casper's innovative deposit control and betting-like mechanisms significantly enhance the security of the blockchain. By requiring validators to have skin in the game, it aligns their interests with the overall health and integrity of the network, reducing the likelihood of malicious activities [36].

3.1.2. PoS and PBFT. In the realm of blockchain consensus mechanisms, the hybridization of PoS with PBFT represents a significant advancement in improving blockchain performance, security, and scalability. This innovative approach effectively merges the unique strengths of both PoS and PBFT, optimizing the overall consensus process within blockchain systems.

3.1.2.1. Integration Benefits

- Enhanced Security and Trust: PoS contributes to security by requiring validators to hold and sometimes lock up a certain amount of cryptocurrency, thus incentivizing honest participation in the consensus process. PBFT further enhances this by allowing a system to continue functioning even if some of the nodes fail or act maliciously, provided that more than two-thirds of the nodes remain honest.
- Increased Scalability: PBFT is known for its efficiency in achieving consensus without the high energy costs associated with traditional PoW systems. When combined with PoS, this hybrid model can handle a larger number of transactions at a faster rate, making it highly scalable.
- Reduced Latency: The PBFT component of the hybrid ensures that transaction confirmations are rapid, significantly reducing the latency that can occur in purely PoS systems, where block creation and validation might take longer due to the stacking and selection process.

3.1.2.2. Operational Dynamics. The hybrid system operates by integrating the stacking mechanism of PoS with the agreement protocol of PBFT. Validators are chosen based on the amount of stake they hold, as in traditional PoS systems. These selected validators then participate in a PBFT-style voting process to confirm blocks, ensuring a dual layer of security and efficiency. This method not only streamlines the validation and block creation process but also ensures that the system remains robust against both external attacks and internal faults.

3.1.2.3. Practical Applications. This hybrid model is particularly advantageous for large-scale enterprise blockchains, where transaction speed and system uptime are critical, and the environmental impact of operations is a concern. By reducing the resource requirements typically associated with PoW systems and combining the trust mechanisms of PoS with the fault tolerance of PBFT, this hybrid consensus model offers a sustainable and efficient solution suitable for a wide range of applications [38].

3.1.3. PBFT and PoA. The integration of PBFT with PoA offers a powerful hybrid consensus mechanism that significantly enhances both security and throughput within permissioned blockchain environments. This combination is particularly effective in systems where reliability and rapid processing are paramount, exemplified by Indonesia's national identity system, the IDNat-Blockchain [39].

3.1.3.1. IDNat-Blockchain: A Case Study. The IDNat-Blockchain is designed to cater to the expansive needs of Indonesia's large population and its complex digital economy. Utilizing a hybrid of PBFT and PoA allows the system to achieve high security and efficient throughput, critical for managing sensitive national data across a diverse and extensive user base.

3.1.3.2. Architectural Design and Benefits

- Security: PBFT helps in mitigating the blockchain's vulnerability to Byzantine failures, where network nodes may fail or act maliciously. It ensures that the blockchain can reach consensus even if some nodes are compromised, which is crucial for maintaining the integrity of a national identity system.
- Throughput: PoA contributes to high transaction throughput by restricting the right to validate and create new blocks to preapproved nodes known as validators. This authority is typically granted based on identity and reputation, which reduces the chances of fraudulent activities and speeds up the consensus process.
- Operational Efficiency: Each layer of the IDNat-Blockchain is specifically tailored to maximize operational efficiency. PBFT's mechanism ensures rapid finalization of blocks, crucial for real-time transaction processing, while PoA's streamlined validation process reduces the computational overhead, enhancing the overall performance of the system.

3.1.3.3. Strategic Implementation for National Identity Management. The hybridization approach within IDNat-Blockchain smartly addresses the unique challenges of administering a national identity system as follows:

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/5821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

- Scalability: Capable of handling large volumes of transactions and user interactions typical in national databases.
- Reliability: Ensures the system remains operational and consistent across various administrative processes, crucial for maintaining public trust and service reliability.

3.1.4. Threshold Relay and PoW. This subsection explores a hybrid consensus mechanism that combines threshold relay with PoW. This hybrid model leverages the rapid transaction validation capabilities of threshold relay alongside the robust security and block finalization features of PoW, creating a system that optimizes both speed and security.

3.1.4.1. Key Features

- Threshold Relay: Utilizes a method where a predefined threshold of validators must agree on a transaction before it moves forward. This approach significantly speeds up the validation process by reducing the number of confirmations needed [40, 41].
- PoW: Ensures the finalization of blocks through computational work, thereby securing the blockchain against alterations and providing a trustless system where no single party has control over the entire chain [29, 42].

The integration of these two mechanisms allows for faster transactions while maintaining the rigorous security standards required by blockchain technologies.

3.1.4.2. Verifiable Chain Relay: Verilay. Verilay is a protocol designed to enhance the interoperability and security of transactions across different PoS blockchains. It plays a crucial role in enabling the seamless transfer of information and assets between disparate blockchain networks, thereby fostering the growth and scalability of the blockchain ecosystem [43].

3.1.4.3. Operational Highlights

- Interoperability Focus: Verilay prioritizes interoperability among PoS blockchains, allowing for fluid communication and asset transfer across networks, essential for the expansion and integration of various blockchain applications [44, 45].
- Security Measures: The protocol incorporates several security measures to safeguard against potential cyber threats. By employing advanced cryptographic methods and consensus mechanisms, Verilay ensures the integrity and trustworthiness of the data relay process [46].
- Scalability and Efficiency: Discusses the protocol's capacity to enhance the scalability and operational efficiency of cross-chain communications, facilitating quicker and more reliable data exchange [43, 47].

3.1.4.4. Potential Use Cases

- Decentralized Finance (DeFi): Verilay can significantly impact DeFi by enabling more secure and efficient multichain interactions, crucial for various financial applications such as loans, swaps, and more complex financial instruments [48, 49].
- Asset Transfers: Facilitates asset transfers between chains, pivotal for token swaps, NFT exchanges, and other asset classes requiring reliable cross-chain functionality [50, 51].
- Cross-Chain Applications: Supports a wide range of applications that benefit from enhanced security and interoperability, such as supply chain tracking, multichain governance systems, and cross-chain data verification [52, 53].

3.1.5. Hedera Consensus Algorithm. The Hedera consensus algorithm is specifically designed for multiaccess edge computing (MEC) networks. It offers permissionless operation to enhance security, decentralization, scalability, and environmental sustainability. Hedera uniquely integrates a permissionless proof-of-capacity algorithm with a permissioned asynchronous Byzantine algorithm, resulting in a robust hybrid blockchain consensus mechanism.

3.1.5.1. Performance Evaluation. To rigorously assess Hedera's performance, a prototype system was developed and deployed. The evaluation focused on several critical metrics as follows:

- Fairness: The Hedera algorithm promotes equitable participation among all nodes, preventing dominance by any single node.
- Throughput and scalability Hedera achieves impressive throughput and scalability, outperforming traditional blockchain systems [54, 55].
- Latency: Hedera maintains low latency in transaction processing, enhancing user experience and system responsiveness.
- Resource Consumption: Compared to PoW-based systems, Hedera significantly reduces resource consumption, aligning with sustainability goals [56, 57].
- MEC Applications: The hybrid consensus model is particularly well-suited for MEC environments, where scalability and low latency are paramount [52, 58].

3.1.5.2. Security Analysis. The robustness of the Hedera algorithm against various potential security threats was also thoroughly analyzed as follows:

- Resilience to Attacks: The system demonstrates strong defenses against Sybil attacks, nothing-at-stake attacks, selfish mining, and message hijacking, ensuring a secure blockchain environment.
- Liveness: Hedera exhibits excellent liveness properties, maintaining consistent and reliable operations under various conditions.

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Experimental results confirm that the Hedera algorithm meets and exceeds performance standards required for contemporary blockchain applications, particularly in MEC environments. Its ability to combine high-throughput and low-resource consumption while maintaining exceptional security and reliability represents a significant leap forward in blockchain technology [59].

3.1.6. Honesty-Based Distributed Proof-of-Authority. This is a novel consensus mechanism, Honesty-Based Distributed Proof-of-Authority, specifically designed for blockchain-based IoT systems. Honesty-Based Distributed Proof-of-Authority merges the robust security features of PoW with the operational efficiency of PoA, creating a mechanism that balances scalability with fast confirmation times [60].

3.1.6.1. Integration and Performance Evaluation

- Scalability and Efficiency: By integrating PoA, Honesty-Based Distributed Proof-of-Authority achieves significant reductions in confirmation times and energy usage, aligning with findings from prior studies on scalable IoT consensus mechanisms [61, 62].
- Security and Privacy: Honesty-Based Distributed Proof-of-Authority addresses common IoT security challenges such as Sybil attacks and data integrity issues, aligning with blockchain solutions proposed in [63, 64].
- Energy Efficiency: The testbed results align with earlier research emphasizing the importance of energy-efficient consensus algorithms for IoT networks [65, 66].

3.1.6.2. Results and Findings

- Performance: The results indicate that Honesty-Based Distributed Proof-of-Authority significantly reduces transaction confirmation time and power consumption compared to traditional PoW systems, underscoring its efficiency.
- Security: The security analysis confirms Honesty-Based Distributed Proof-of-Authority capability to withstand common blockchain threats, ensuring robust network resilience.

3.1.6.3. Experimental Setup and Implementation

- Testbed Configuration: Honesty-Based Distributed Proof-of-Authority was evaluated using a custom-built testbed that included 30 different IoT devices, such as Raspberry Pis, ESP32, and ESP8266. These devices were selected for their cost-effectiveness and varying computational capabilities.
- Energy and Performance Metrics: Performance measurements focused on energy consumption, devices' battery life, and hash power. Notable findings included hash per joule (h/J) rates of 13.8 Kh/J for Raspberry Pis, 54 Kh/J for ESP32 devices, and 22.4 Kh/J for ESP8266 devices. These metrics illustrate the energy efficiency of Honesty-Based Distributed Proof-of-Authority across diverse hardware platforms [60].

3.1.6.4. Contributions and Implications

- Innovation in IoT Blockchain: This study not only designs and implements Honesty-Based Distributed Proof-of-Authority but also validates its effectiveness in real-world scenarios, demonstrating significant improvements in energy efficiency and transaction speed.
- Suitability for IoT Applications: The successful deployment and testing of Honesty-Based Distributed Proof-of-Authority confirm its practical applicability and superiority in IoT blockchain contexts, where maintaining a balance between security, power consumption, and operational efficiency is paramount [60].

3.1.7. Microchain: Hybrid Proof-of-Credit (PoC) and Voting-Based Chain Finality (VCF) Protocol. Microchain introduces a novel hybrid consensus mechanism designed specifically for IoT systems, combining PoC with a VCF protocol. The PoC component in Microchain ensures fairness by credit-based block proposal eligibility, aligning with lightweight IoT blockchain strategies described in [67, 68].

3.1.7.1. Consensus Mechanism Overview

- PoC: At its core, PoC is a variant of the PoS protocol that evaluates participants' eligibility to propose new blocks based on their credit assignment within the network. This method ensures a fair and equitable distribution of proposing rights, reducing the risk of dominance by any single node.
- VCF: This protocol ensures blockchain stability by finalizing the block history through a decentralized voting process among nodes. It resolves conflicts between checkpoints and selects a unique, definitive chain of blocks. By requiring supermajority agreement, VCF enhances security, consistency, and resistance to forks, ensuring robustness even in the presence of adversarial attacks. Its efficient design also reduces latency and improves transaction finality.

3.1.7.2. Technical Implementation

- Committee Selection: Microchain utilizes a cryptographic sortition algorithm, coupled with a bias-resistant randomness protocol, to select a random subset of nodes known as the "final committee." The members of this committee are responsible for executing the consensus protocol.
- Security and Scalability: The use of VRF-based cryptographic sortition enhances both security and scalability, as highlighted in [69, 70]. This unpredictability prevents potential attackers from manipulating or predicting the choice of nodes that participate in the consensus process.

3.1.7.3. Performance Enhancements

- Reduced Communication Complexity: By limiting the consensus process to a small group of validators within

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

the final committee, Microchain significantly cuts down on communication overhead, a critical factor in maintaining high performance in distributed networks.

- Improved Transaction Performance: The hybrid PoC-VCF mechanism allows Microchain to achieve faster confirmation times and higher throughput, making it an ideal solution for IoT systems that require quick and reliable transaction processing.

3.1.7.4. Implications for IoT Systems. Microchain's lightweight architecture addresses the resource constraints of IoT systems, echoing findings in [71, 72]. Its lightweight and efficient consensus mechanism makes it particularly effective in environments where resources such as bandwidth and energy are limited [72].

3.1.8. Proof of Luck (PoL) Integrated With PBFT: Enhancing Efficiency in Blockchain Consensus. This paper presents a hybrid consensus mechanism that integrates PoL with PBFT to optimize energy efficiency during the block validation process. By combining these two approaches, the system aims to achieve both security and reliability while significantly reducing power consumption, which is traditionally high in PoW systems [73].

3.2. Hybrid Consensus Overview

- Initial Process: The hybrid mechanism initially employs both proof-based and voting-based consensus. The system determines the more efficient process—either PoL or PBFT—based on the time taken for solving and validating blocks. The faster method then becomes the primary mechanism for subsequent rounds.
- Miner Selection and Validation: Miners are initially selected via the PoL method, which is primarily proof-based. To ensure the integrity of the selected miner, the PBFT voting-based approach is then used for validation. This validated miner is authorized to add transactions to the blockchain network for the next 100 rounds, enhancing efficiency by minimizing the repetitive competition typical in proof-based systems [17].

3.2.1. Performance and Environmental Impact

- Energy Consumption: Comparative studies within this paper reveal that energy consumption is significantly lower in PoL integrated with PBFT than in traditional PoW, PoS, and even DPoS systems. This reduction is primarily due to eliminating redundant competitions among miners, as the majority of miners vote once for validating nodes, thereby saving energy.
- Environmental Benefits: The reduction in energy consumption directly decreases electronic waste and environmental impact, making this hybrid approach particularly beneficial for applications requiring sustainable solutions.

3.2.2. Applications and Security

- Real-time Vehicular Communication: The proposed hybrid consensus mechanism is especially suited for real-time vehicular communication systems, where rapid and secure transaction validation is crucial for safety and operational efficiency [74].
- Security and Attack Resistance: The mechanism is designed to resist various security threats prevalent in blockchain networks, thereby safeguarding information integrity and access.

3.2.3. Empirical Evaluation

- Experimental Results: Performance measurements from different block sizes within the blockchain network demonstrate that the hybrid approach outperforms existing algorithms in terms of energy efficiency and computation time.
- Comparative Analysis: Trends in energy consumption and computation time for 10 rounds, when compared with existing algorithms, show that the proposed hybrid method offers substantial improvements in both energy saving and processing speed.

3.3. Comparison Hybrid Consensus Algorithms. Hybrid consensus mechanisms are increasingly utilized within blockchain networks due to their ability to synergize different algorithms, thereby optimizing performance across various dimensions. This section presents Table 3, which outlines the combination of algorithms, their distinctive characteristics, and probable applications for each hybrid consensus model. These hybrid models are specifically designed to address unique challenges and enhance specific aspects of blockchain consensus, offering tailored solutions to meet the diverse requirements of blockchain applications. Table 3 provides an in-depth comparison of different hybrid consensus algorithms, highlighting their unique attributes and the critical factors to consider for each.

Table 3 illustrates how each hybrid model combines the strengths of different consensus mechanisms to optimize blockchain functionality. For instance, the Honesty-Based Distributed Proof-of-Authority hybrid leverages a scalable work consensus protocol tailored for IoT applications. By combining the Honesty-Based Distributed Proof-of-Authority with scalability features, this model addresses the specific needs of IoT systems, such as lightweight operation, high security, and efficient resource utilization, making it suitable for environments with constrained devices and real-time requirements.

3.4. Classification of Hybrid Consensus Mechanisms. Hybrid consensus mechanisms can be categorized based on three primary criteria: combination type, performance focus, and application domain. This multidimensional approach ensures a thorough understanding of their functional and operational attributes.

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Table 3: Comparison between different hybrid consensus algorithms.

Reference	Consensus hybrid	Characteristics	Strengths	Weaknesses
[36]	PoW + PoS	Energy-intensive PoW for block creation, PoS for transaction validation within blocks	Security of PoW, energy efficiency of PoS	Potential centralization, complex implementation
[38]	PoS + PBFT (Casper)	Stake-based validation, fault tolerance combining PoS security with PBFT rapid consensus attainment	Enhanced security, speed and finality, decentralization	Complexity, scalability challenges with node growth
[75]	PBFT + PoA	PBFT for fast consensus, PoA for enhanced throughput and security in permissioned chains	Fast consensus, enhanced throughput and security	Limited decentralization, permissioned nature
[43]	Threshold relay + PoW	Threshold relay for transaction validation, PoW for block finalization and security	Faster transaction validation, enhanced security	Overhead in threshold setup, energy consumption
[59]	Hedera	Permissionless and scalable hybrid blockchain in multiaccess edge computing for IoT	Scalability, permissionless nature	Centralization concerns
[60]	HDPoA	Honesty-based distributed proof-of-authority for IoT–blockchain using a scalable work consensus	Security, scalability	Centralization concerns
[68]	Microchain	Lightweight distributed ledger with a hybrid consensus mechanism for IoT	Efficiency, lightweight nature	Limited scalability
[74]	PoL integrated with PBFT	Robust hybrid consensus mechanism for blockchain-based vehicular communication	Robustness, suitability for vehicular communication	Limited scalability
[76]	DAG + PoS	Utilizes DAG's scalability with PoS validation for high transaction throughput and low latency	Scalability, low latency, suitability for IoT	Relatively new, security concerns

iis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/5821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

3.4.1. By Combination Type

- PoW and PoS: Combines PoW's robust security with PoS's energy efficiency to balance transaction throughput and energy consumption. *Example: Ethereum's transition to PoS-based Casper while retaining elements of PoW* [77].
- PoS and BFT (Byzantine Fault Tolerance): Integrates PoS's stake-based governance with BFT to enhance security and performance. *Example: Tendermint, used in Cosmos* [78].
- DAG and PoS: Utilizes DAG's scalability with PoS validation for high transaction throughput and low latency. *Example: IOTA for IoT networks* [79].
- PBFT and PoA: Combines PBFT's consensus speed with PoA's identity-based validation, enhancing scalability for permissioned blockchains. *Example: Hyperledger Fabric* [80].

3.4.2. By Performance Focus

- Scalability-Enhanced Hybrids: Optimized for handling large transaction volumes without compromising network speed. *Example: DAG + PoS hybrids, such as IOTA* [79].
- Security-Enhanced Hybrids: Focused on addressing vulnerabilities like Sybil attacks, double-spending, and partitioning issues. *Example: Microchain for mitigating common attack vectors* [81].
- Energy Efficiency Hybrids: Aim to reduce energy consumption while maintaining performance. Example: PoW + PoS hybrids, such as Ethereum's Casper model [77].

3.4.3. By Application Domain

- Financial Services: Tailored for high-security, high-volume transaction processing. *Example: Casper's implementation for Ethereum 2.0* [77].
- IoT: Designed for low-power, intermittently connected devices. *Example: Honesty-Based Distributed Proof-of-Authority for lightweight IoT consensus* [60].
- Supply Chain Management: Optimized for traceability and data integrity. *Example: VeChain's hybrid consensus for supply chain applications* [82].

By adopting this classification and linking each category to specific hybrid models, we provide a comprehensive framework to evaluate the adaptability, efficiency, and security of hybrid consensus mechanisms across different blockchain environments. This approach enables stakeholders to make informed decisions tailored to their operational needs.

4. Hybrid Consensus Mechanisms: Key Categories and Applications

This section examines the critical aspects of hybrid consensus mechanisms, categorized into six primary classes: validation, IoT, real-time processing, application suitability, security, and implementation. Each category is explored in depth, showcasing how hybrid mechanisms address specific needs within blockchain technology. We present Table 4 as a comprehensive overview of several hybrid consensus mechanisms used in blockchain systems, highlighting their distinctive configurations and the specific problems they address. Each entry in the table details the innovative contributions of different hybrid models, outlines their methodology, and discusses their limitations and the technologies employed. This structured format facilitates not only a better understanding of each mechanism's unique attributes, but also illustrates how they can be applied in practice to enhance blockchain performance and security.

Table 4 summarizes the various classes of hybrid consensus mechanisms, highlighting their distinguishing characteristics, functionality, and operational frameworks based on six critical aspects: validation, IoT, real-time processing, application suitability, security, and implementation. The details of these aspects are discussed in the following subsections, providing a comprehensive understanding of the hybrid consensus landscape and facilitating informed discussions and analyses within the domain of decentralized systems and blockchain technology.

4.1. Validation in Hybrid Consensus. Mechanisms validation is crucial for maintaining the blockchain's integrity, involving multiple steps tailored to each consensus mechanism. Below is a comprehensive table "Table 5" that combines the strengths and weaknesses of various hybrid consensus mechanisms across multi-step aspects of validation.

By evaluating these multistep validation aspects, one can choose the optimal consensus mechanism based on the specific requirements of the blockchain application. Each hybrid mechanism offers a different balance of security, efficiency, scalability, and decentralization, making it crucial to align the chosen mechanism with the goals and constraints of the project. For example:

- PoW + PoS: Offers strong security and energy efficiency but faces potential centralization and complexity.
- Casper (PoS + PBFT): Provides enhanced security and fault tolerance with rapid consensus but struggles with complexity and scalability.
- Threshold Relay + PoW: Provides strong security and thorough block integrity checks but at the cost of high energy consumption and resource demands.
- Hybrid Delegated Proof of Authority: Ensures quick and secure block verification with scalability benefits but faces centralization and complexity challenges.
- Hedera Hashgraph: Excels in scalability and decentralized verification but has potential centralization risks and implementation complexities.
- PBFT + PoA: Ensures fast and secure verification but suffers from limited decentralization.

Understanding the trade-offs in each hybrid consensus mechanism is essential for selecting the most appropriate one for maintaining blockchain integrity. Each mechanism

Table 4: List of hybrid consensus mechanism papers.

Paper title	Problem	Contribution	Methodology		Limitations	Used tech
			Tools	Evaluation metrics		
Hedera: A permissionless and scalable hybrid blockchain consensus algorithm in multi-access edge computing for IoT [59]	Challenges with consensus algorithm in edge networks, limited resources of edge nodes, expanding network scale	Proposes Hedera consensus algorithm, combining proof-of-capacity, and asynchronous Byzantine algorithms	• Permissionless proof-of-capacity • Permissioned asynchronous Byzantine	• Scalability • Fairness • Latency	• Limited resources of edge nodes • Expanding network scale	Hedera prototype deployed on Amazon and Alibaba cloud
Tree-chain: A fast lightweight consensus algorithm for IoT applications [83]	Conventional blockchains have limited throughput and high transaction delays. Existing consensus algorithms are computationally expensive	Proposed tree-chain consensus algorithm for IoT applications, introduced two levels of randomization among validators	• Tree-chain consensus algorithm based on hash function output • Random consensus code allocation for validator selection	• Processing time • Delay • Performance • Number of potential validators	Limited throughput and high transaction delays are common limitations of conventional blockchains, which tree-chain aims to address	Java programming language
CBCIoT: A consensus algorithm for blockchain-based IoT applications [84]	IoT applications require a low-latency consensus mechanism	• Proposed CBCIoT consensus algorithm for blockchain-based IoT applications. • Improved scalability in terms of validation and verification rate	CBCIoT, a consensus algorithm for blockchain-based IoT applications	• Accessibility • Decentralization • Throughput • Scalability • Verification speed	• IoT applications require low-latency consensus mechanism • Slight delay is acceptable for IoT devices	Java-based simulation
Design and implementation of hybrid consensus mechanism for IoT-based healthcare system security [85]	The reliability problem still exists in blockchain technology. The proposed HCM aims to overcome trust- worthiness issues	• Implementation of a blockchain- based HCM for electronic healthcare system (EHS) security. • Comparison of HCM with PoXR	• HCM • PoXR	• CPU and memory consumption • Latency • Security • Scalability	• HCM in terms of handling different types of attacks or malicious activities are not discussed in detail. • No comprehensive evaluation of HCM's performance in scalability, efficiency, and security	C++ software plat-form
Securing IoT–Blockchain applications through honesty-based distributed proof of authority consensus algorithm [60]	• Long confirmation time of PoW • Lack of security in existing consensus mechanisms	Proposed a novel consensus mechanism called honesty-based distributed proof-of-authority (HDPoA). Demonstrated the suitability and security of HDPoA for blockchain-based IoT applications	• PoA • PoW	• Confirmation time • Power consumption • Security aspects	• Utilization of diverse IoT devices. • Large-scale and long-term testing. • Testing with different connection protocols	Raspberry Pi 3 model B+ (1.4 GHz 64-bit quad-core processor) and two ESP32 microcontrollers

iis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/iis/5821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Table 4: Continued.

Paper title	Problem	Contribution	Methodology		Limitations	Used tech
			Tools	Evaluation metrics		
Microchain: A hybrid consensus mechanism for lightweight distributed ledger for IoT [68]	• Challenges in integrating blockchain technology into resource-constrained IoT platforms. • Power-intensive and low-throughput consensus mechanism in existing blockchains	• Proposed Microchain as a hybrid consensus mechanism • Implemented and tested a proof-of-concept prototype	• Hybrid proof-of-credit (PoC)–voting-based chain finality (VCF) consensus protocol • Bias-resistant randomness protocol, cryptographic sortition algorithm	• Latency • Throughput • Performance • Security	Committee selection could improve scalability of Microchain, more investigation is needed to evaluate how committee selection algorithm scales to network size	Implemented in Python
HDPoA: Honesty-based distributed proof of authority via scalable work consensus protocol for IoT–blockchain applications [60]	• Integrating blockchain into IoT systems presents challenges. • Designing a suitable consensus protocol for IoT systems	• Introducing honesty-based distributed proof-of-authority (HDPoA) consensus protocol • Conducting performance and security analysis of HDPoA	• HDPoA • Integration of PoW	• Energy consumption • Hash power • Performance	Not discuss the scalability of the HDPoA protocol in terms of the number of IoT	Raspberry Pis, ESP32, and ESP8266
Hybrid consensus approach for blockchain-based vehicular communication [74]	The paper proposes a hybrid consensus approach for blockchain-based vehicular communication, integrating PoL and PBFT consensus to improve data security and reliability	• Proposed a blockchain-based method for vehicular communication • Integrated PoL and PBFT consensus for better results	• Hybrid consensus: PoL and PBFT • Blockchain-based method for vehicular communication	• Security • Reliability • Reduces energy consumption and e-waste	Not provide a detailed analysis of the performance and scalability of the proposed hybrid consensus approach	The block manager (BM) is a block node installed at roadside areas to monitor and control vehicular communication

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/5821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Table 4: Continued.

Paper title	Problem	Contribution	Methodology		Limitations	Used tech
			Tools	Evaluation metrics		
Hybrid consensus algorithm based on modified proof-of-probability and DPoS [86]	A hybrid consensus algorithm based on modified proof-of-probability and delegated PoS that significantly weakens the ability of supernodes in the DPoS algorithm to conduct monopoly behavior or other malicious behaviors	• Proposed hybrid consensus algorithm based on modified proof-of-probability and delegated proof-of-stake. • Increased security, efficiency, and decentralization of blockchain systems	• Modified proof-of-probability consensus algorithm • Delegated PoS consensus algorithm	• Security • Efficiency • Decentralization • Scalability	• Optimization of mechanisms: The optimization of the waiting time mechanism and the bit adjustment algorithm will be the main research directions. • Sublinear function impact: The introduction of a sublinear function has resulted in nodes holding a small number of tokens having a greater voting weight than a single node holding a large number of tokens. This will be an area of focus	Python socket
Grape: Efficient hybrid consensus protocol using DAG [87]	Proposes grape, an efficient hybrid consensus protocol using a directed acyclic graph structure to address challenges faced by other hybrid consensus schemes. Grape is an efficient hybrid consensus protocol using directed acyclic graph	Grape achieves high transaction throughput with instant confirmation	Utilizes classic Byzantine fault-tolerant protocol with a rolling committee uses directed acyclic graph structure for efficient hybrid consensus protocol	• Throughput • Latency	• Hybrid consensus schemes using Nakamoto single chain have low throughput and poor scalability. • The committee's internal consensus process is interrupted during rotation	Prototype and make the experimental evaluation
AI-enabled consensus algorithm in human-centric collaborative computing for internet of vehicle [88]	AI-enabled consensus algorithm with vehicle features, combining vehicle-based metrics and neural networks, which effectively solves the situation that the primary node vehicle drops off in collaborative IoV	Ensured safety, stability, and effectiveness of collaborative vehicle networking while saving energy costs	• AI-enabled consensus algorithm with vehicle features. • Integral model and hierarchical classification method combined with BP neural network	• Delay • Energy consumption	• Classical consensus algorithms are not adaptable to the immediacy and flexibility of vehicles. • Mass computing required by classical consensus algorithms increases communication overhead	Software environment

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/5821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Table 4: Continued.

Paper title	Problem	Contribution	Methodology		Limitations	Used tech
			Tools	Evaluation metrics		
DRBFT: Delegated randomization Byzantine fault tolerance consensus protocol for blockchains [89]	Delegated randomization Byzantine fault tolerance consensus protocol named DRBFT based on practical PBFT to enhance the efficiency and reliability of the consensus procedure	RS based on hash functions to select representative nodes from all nodes in the blockchain. The distribution of the outputs of RS algorithm is proven to be statistically indistinguishable from the uniform distribution, which ensures the fairness of selection	• RS algorithm • DRBFT scheme	• Efficiency • Impartiality • Reliability	• Less comparison typifies and factors with DRFT	Prototype implementation
Distributed hybrid double-spending Attack prevention mechanism for proof-of-work and proof-of-stake blockchain consensuses [90]	Hybrid algorithm that combines PoW and PoS mechanisms to prevent double-spending attacks in blockchain consensuses	• Proposed a hybrid algorithm combining PoS and PoW mechanisms. • Reduced the possibility of double mining by requiring 100% dominance	• Hybrid algorithm combining PoW and PoS mechanisms. • The algorithm conducts forking to combine PoW and PoS consensuses	• Computational power • Delay • Security	• Delay issues and unsorted block sequences in previous solutions. • Vulnerability to double-spending attacks, particularly the 51% attack	Simulation
A new hybrid consensus protocol: Deterministic proof of work [91]	New hybrid consensus protocol called deterministic proof of work (DPoW) that combines map-reduce PoW mining and practical PBFT verification to achieve scalability, consistency, and decentralization in blockchain networks	Improved scalability and consistency without significant reduction in decentralization	• Deterministic proof of work (DPoW) protocol. • Map-reduce PoW mining algorithm alongside practical PBFT verification	• Scalability • Consistency • Decentralization • Security	• Incorporate a reputation score in the verifier election process, which increases security against attackers	Implement our protocol using the Go language
HotDAG: Hybrid consensus via sharding in the permissionless model [92]	Hybrid consensus protocol based on HotStuff via sharding in the permissionless model, to improve scalability and performance of blockchain	• HotDAG is a hybrid consensus protocol based on HotStuff via sharding in the permissionless model. • Introduces a decentralized and bias-resistant sharding mechanism using the parallel Nakamoto consensus protocol	• HotDAG is a hybrid consensus protocol based on HotStuff via sharding. • Employs the parallel Nakamoto consensus protocol and introduces a scalable BFT protocol	• Scalability • Performance • Security	• Sharding mechanism weakens decentralization or reduces protocol performance. • BFT protocols are unresponsive or have quadratic communication complexities under a Byzantine leader	

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/5821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Table 4: Continued.

Paper title	Problem	Contribution	Methodology		Limitations	Used tech
			Tools	Evaluation metrics		
A hybrid double-layer BFT consensus protocol for large-scale IoT blockchain [93]	Hybrid double-layer BFT consensus protocol for large-scale IoT blockchain, which divides nodes into groups and achieves consensus within each group before reaching an overall consensus among the groups	Proposed hybrid double-layer BFT consensus protocol. Utilized clustering method for energy-efficient communication	• Hybrid double-layer BFT consensus protocol. • Weighted asynchronous Byzantine agreement (WABA)	• Energy consumption • Scalability • Delay	• Limited power and computing capability of IoT devices. • Poor node scalability of PBFT algorithm	Simulation
Hybrid consensus algorithm based on hierarchical authority [94]	Hybrid consensus algorithm based on hierarchical authority, which combines the PBFT algorithm and the Raft algorithm to improve consensus efficiency in hierarchical systems	• Proposed a hybrid consensus algorithm based on hierarchical authority. • Combined PBFT and Raft algorithms to suit hierarchical systems	• Hybrid consensus algorithm based on hierarchical authority. • Combination of PBFT and Raft algorithms	• Delay • Scalability • Fault tolerance	Improved with cryptography technology to solve the Byzantine problem of follower nodes and further strengthen the fault-tolerant ability of the algorithm	Implemented based on Golang language
Hybrid consensus protocols and security analysis for blockchain [95]	Security analysis of hybrid consensus protocols in blockchain systems, analyzing mainstream consensus protocols and their vulnerabilities. It also presents hybrid protocol cases and their security analysis	Focuses on the original consensus protocols for hybridization, the problem that each hybrid case is trying to solve, and the security performance of those hybrid protocols. Each hybrid case shows improvements in preventing certain security attacks	• Classification of mainstream consensus protocols. • Analysis of hybrid protocol cases and their security	• Security • Performance	• Evaluate the security performance of hybrid protocols, statistical analysis on security performance, and applications of hybrid protocols in specific fields	

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/5821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Table 5: Comparative analysis based on validation in hybrid consensus mechanisms.

Mechanism	Multistep validation aspect	Strengths	Weaknesses
PoW + PoS	Transaction verification	Security: PoS enhances security by validating transactions within blocks. Energy efficiency: Reduced energy consumption compared to pure PoW systems	Potential centralization: PoS can lead to centralization if few participants control a significant stake
	Consensus verification	Enhanced security: PoW provides strong security	Energy consumption: High energy requirements
	Block verification	Strong security: Ensures robust block finalization Integrity of blocks: Ensures rigorous verification	Energy consumption: High energy requirements Resource intensive: Slow and resource-heavy verification process
	Network-wide verification	Security: Strong security from PoW Energy efficiency: PoS enhances energy efficiency	Potential centralization: Centralization risks with PoS Complex implementation: Complexity in combining PoW and PoS
Casper (PoS + PBFT)	Transaction verification	Enhanced security: Stake-based validation ensures secure transactions Speed and finality: PBFT allows for rapid transaction finality Decentralization with efficiency: Efficient consensus process that remains decentral	Complexity: Integration of PoS with PBFT increases complexity Scalability challenges: Communication overhead can increase as the network grows
	Consensus verification	Enhanced security: Strong security and fault tolerance Speed and finality: Rapid consensus	Complexity: Complex to implement and maintain Scalability challenges: Issues with growing node numbers
	Block verification	Enhanced security: Ensures secure block verification Speed and finality: Rapid block finality	Complexity: Challenges in implementing the combined consensus mechanism Scalability challenges: Issues with growing node numbers
	Network-wide verification	Enhanced security: Strong security and fault tolerance Speed and finality: Rapid consensus	Complexity: Complex to implement and maintain Scalability challenges: Issues with growing node number
Threshold relay + PoW	Transaction verification	Faster transaction validation: Threshold relay accelerates transaction validation Enhanced security: PoW ensures robust security for block finalization	Overhead in threshold setup: Additional computational requirements Energy consumption: PoW is energy intensive
	Consensus verification	Enhanced security: PoW provides strong security	Energy consumption: High energy requirements
	Block verification	Enhanced security: Strong security through PoW Integrity of blocks: Ensures rigorous verification	Energy consumption: High energy requirements Resource intensive: Slow and resource-heavy verification process
	Network-wide verification	High throughput: Facilitates high throughput and parallel processing of data transactions Strong security: PoW provides robust security	Energy consumption: High energy requirements Overhead: Threshold setup requires additional computational resources

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/5821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Table 5: Continued.

Mechanism	Multistep validation aspect	Strengths	Weaknesses
HDPoA	Transaction verification	Low energy consumption: Efficient for IoT devices Quick finality: Rapid transaction processing	Centralization: Preselected validators can lead to centralization Complexity: Combining PoA with periodic PoW increases complexity
	Consensus verification	Security: PoA combined with periodic PoW enhances security Scalability: Efficient consensus mechanism	Centralization concerns: Reliance on preselected validators can lead to centralization Complexity: Integration of PoA with periodic PoW adds complexity
	Block verification	Security: PoA and periodic PoW ensure secure block verification Scalability: Efficient handling of transaction volume	Centralization concerns: Potential for centralization with PoA Complexity: Challenges in implementing the combined consensus mechanism
	Network-wide verification	Scalability: Efficient handling of transaction volume Security: PoA combined with periodic PoW enhances security	Centralization concerns: Potential for centralization with PoA Complexity: Challenges in implementing the combined consensus mechanism
Hedera Hashgraph	Transaction verification	Scalability: High transaction throughput Permissionless nature: Decentralized consensus process	Centralization concerns: The governance model can introduce centralization risks Complexity: Implementation complexity of Hashgraph
	Consensus verification	Scalability: High transaction throughput Permissionless nature: Decentralized consensus process	Centralization concerns: Governance model can introduce centralization risks Complexity: Implementation complexity of hashgraph
	Block verification	Scalability: High throughput for block verification Permissionless nature: Decentralized verification process	Centralization concerns: Risks due to the governance model Complexity: Complex implementation of hashgraph
	Network-wide verification	Scalability: High throughput for network-wide verification Permissionless nature: Decentralized consensus process	Centralization concerns: The governance model risks centralization Complexity: Sophisticated hashgraph implementation
PBFT + PoA	Transaction verification	Fast and secure: Quick consensus and high throughput	Fast and secure: Quick consensus and high throughput
	Consensus verification	Fast and secure: Quick consensus with trusted authorities High throughput: Efficient handling of transactions	Limited decentralization: PoA can limit decentralization Governance: Reliance on trusted authorities introduces centralization risk
	Block verification	Secure and fault-tolerant: Ensures secure consensus on energy transactions Trusted authorities: PoA designates trusted validators	Limited decentralization: Permissioned nature limits decentralization Governance: Reliance on trusted authorities introduces centralization risk
	Network-wide verification	Fast and secure verification: Quick consensus and high throughput	Limited decentralization: Permissioned nature limits decentralization

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/5821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

has unique strengths and weaknesses across transaction verification, consensus verification, block verification, and network-wide verification. By evaluating these factors, one can choose the optimal consensus mechanism based on the specific requirements of the blockchain application.

4.2. IoT Applications. Hybrid consensus mechanisms enhance IoT applications by providing scalable, efficient, and secure transaction validations suitable for resource-constrained environments. Below is a detailed comparison of various mechanisms tailored for IoT applications, as shown in Table 6.

4.2.1. Example Applications

1. Microchain for IoT:
   - Strengths: Lightweight and scalable, Microchain is ideal for real-time operations without compromising security.
   - Use Case: Suitable for IoT applications requiring minimal resource usage, such as environmental monitoring systems.
2. Hybrid Delegated Proof of Authority for IoT:
   - Strengths: Ensures low energy consumption and fast transaction finality, making it efficient for IoT devices.
   - Use Case: Critical for IoT applications needing quick finality, such as smart home automation systems.
3. Casper for IoT Supply Chain:
   - Strengths: Provides secure tracking of goods, with PoW ensuring security and PoS enabling energy-efficient consensus.
   - Use Case: Optimal for supply chain management involving IoT devices, ensuring transparent and secure tracking.
4. PBFT + PoA for Smart Grids:
   - Strengths: Ensures secure and fault-tolerant consensus on energy transactions, with trusted authorities validating transactions.
   - Use Case: Applicable in IoT-based smart grid systems for secure and efficient energy transaction validation.
5. Threshold Relay + PoW for Data Marketplaces:
   - Strengths: Facilitates high throughput and parallel processing of data transactions, with strong security guarantees.
   - Use Case: Ideal for IoT data marketplaces, enabling secure and efficient data exchange.
6. Hedera Hashgraph for Smart Cities:
   - Strengths: Ensures fast and reliable data sharing, supporting a large number of devices in real-time communication.
   - Use Case: Suitable for smart cities and industrial IoT applications requiring reliable and fast data coordination.

Hybrid consensus mechanisms provide tailored solutions for various IoT applications by addressing specific needs such as scalability, efficiency, and security. By selecting the appropriate mechanism based on the application requirements, IoT systems can achieve optimal performance and reliability.

4.3. Real-Time Processing. Real-time processing is essential for applications requiring immediate data validation and consensus. This part compares various hybrid consensus mechanisms based on their real-time processing capabilities. Table 7 presents a comparative analysis of each mechanism's efficiency, outlining the advantages that support rapid processing and the limitations that may hinder performance under time-sensitive conditions.

Each of these hybrid mechanisms presents unique strengths and weaknesses, making them suitable for different blockchain applications based on specific requirements. For example:

- Casper (PoS + PoW): Combines PoW security with PoS efficiency, offering quick consensus but facing potential centralization and complexity.
- PoS + PBFT: Provides rapid transaction finality and energy efficiency, with complexity and scalability challenges.
- PBFT + PoA: Ensures fast and secure consensus with high throughput, limited by decentralization and governance concerns.
- Threshold Relay + PoW: Facilitates high throughput with strong security, hindered by energy consumption and overhead.
- Hedera Hashgraph: Offers rapid processing and scalability, with potential centralization risks and implementation complexity.
- Hybrid Delegated Proof of Authority: Ensures low energy consumption and quick finality, facing centralization and complexity issues.
- Microchain: Designed for IoT with lightweight and scalable operations, potentially complex to integrate and scale.
- PoL + PBFT: Provides high efficiency and secure consensus, with complexity and governance limitations.

4.4. Application Suitability. Different hybrid consensus mechanisms are suited for various applications based on their unique capabilities as follows:

- Casper (PoS + PoW): Designed for environments where security and energy efficiency are paramount. *Example: Suitable for public and permissionless networks, such as Ethereum's transition to PoS-based Casper* [77].

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Table 6: Comparison of blockchain mechanisms for IoT applications.

Mechanism	Strengths	Suitable IoT application
Microchain [81]	• Lightweight solution: Supports real-time operations without compromising security or scalability. • Designed for IoT: Tailored to the needs of IoT environments	Real-time IoT operations requiring minimal resource usage
HDPoA (hybrid delegated proof of authority) [60]	• Low energy consumption: Critical for the efficiency and functionality of IoT devices. • Fatt Transaction finality: Ensures rapid processing	Energy-efficient IoT applications needing quick finality
Casper (PoS + PoW) [77]	• Secure tracking: Ensures secure and transparent tracking of goods in a supply chain. • Energy efficiency: PoS enables energy-efficient consensus among IoT devices	Supply chain management involving IoT devices
PBFT + PoA [80]	• Secure and fault-tolerant: Ensures secure consensus on energy transactions. •Trusted authorities: PoA designates trusted validators	IoT-based smart grid systems for secure energy transactions
Threshold relay + PoW [43]	• High throughput: Facilitates high throughput and parallel processing of data transactions. • Strong security: PoW provides necessary security guarantees	IoT data marketplaces for efficient and fair data exchange
Hedera hashgraph [96]	• Fast and reliable: Enables real-time communication and consensus on data integrity. • Scalable: Supports a large number of devices	Smart cities and industrial IoT requiring reliable data sharing

iis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/iis/5821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Table 7: Comparative analysis of blockchain mechanisms based on real-time processing.

Mechanism	Strengths	Weaknesses
Casper (PoS + PoW) [77]	• Quick consensus: Combines PoW security with PoS efficiency. • Energy efficiency: PoS reduces energy consumption	• Complexity: Integrating PoW with PoS can be complex • Potential centralization: PoS can lead to centralization if few participants control a significant stake
PoS + PBFT [78]	• Rapid transaction finality: PBFT allows for quick consensus • Energy efficient: PoS minimizes energy usage	• Complexity: Combining PoS with PBFT increases implementation complexity • Scalability: PBFT may face challenges as network size grows
PBFT + PoA [80]	• Fast and secure: Quick consensus with trusted authorities • High throughput: Efficient handling of transactions	• Limited decentralization: PoA can limit decentralization • Governance: Reliance on trusted authorities introduces centralization risks
Threshold relay + PoW [43]	• High throughput: Facilitates fast transaction validation • Strong security: PoW provides robust security	• Energy consumption: PoW is energy-intensive • Overhead: Threshold setup requires additional computational resources
Hedera hashgraph [96]	• Rapid processing: Ensures fast and reliable data sharing • Scalable: Supports large numbers of devices	• Centralization concerns: Governance model may introduce centralization risks • Implementation complexity: Sophisticated hashgraph implementation
HDPoA [60]	• Low energy consumption: Efficient for IoT devices • Quick finality: Rapid transaction processing	• Centralization: Preselected validators can lead to centralization • Complexity: Combining PoA with periodic PoW increases complexity
Microchain [81]	Lightweight solution: Designed for IoT, supporting real-time operations. Scalable: Maintains security without compromising scalability	Implementation: May involve complex integration and maintenanceScalability: Potential challenges as network size increases
PoL + PBFT [59]	• High efficiency: PoL ensures quick and fair leader selection • Secure consensus: PBFT provides fault tolerance and rapid finality	• Complexity: Integration of PoL with PBFT can be complex • Governance: PBFT scalability may be limited by communication overhead

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/5821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

- Microchain and Honesty-Based Distributed Proof-of-Authority: Optimized for IoT applications, where the integration of blockchain technology needs to be both effective and economical. *Example: Microchain supports real-time IoT operations, while Honesty-Based Distributed Proof-of-Authority ensures low energy consumption for smart home systems* [60, 81].
- Hedera Hashgraph: Offers robust security, fairness, and scalability, making it ideal for decentralized applications requiring distributed governance or tokenization. *Example: Used by enterprises for tokenized assets and governance systems* [96].
- PoS + PBFT and PBFT + PoA: Provide high throughput and low latency, making them suitable for permissioned networks or consortia. *Example: Hyperledger Fabric's implementation for supply chain management* [80].
- Threshold Relay + PoW: Combines PoW's security with efficient transaction processing, suitable for IoT data marketplaces or DeFi applications [43].

When considering the application suitability of the different hybrid consensus mechanisms discussed above, it becomes evident that each mechanism has unique strengths tailored to specific types of decentralized applications as follows:

- Security-Driven Applications: Casper (PoS + PoW) and Threshold Relay + PoW excel in applications where security and resistance to Sybil attacks are critical. These mechanisms are ideal for public and permissionless blockchain networks, such as DeFi or cryptocurrency platforms.
- Real-Time Updates and Low Latency: Mechanisms combining PoS with BFT, such as PoS + PBFT and PBFT + PoA, provide high throughput and fast transaction finality. They are well-suited for real-time processing in permissioned networks, such as healthcare data management or financial settlements.
- IoT and Lightweight Applications: Microchain and Honesty-Based Distributed Proof-of-Authority are tailored for IoT environments, supporting low-power devices with minimal resource consumption. These mechanisms are effective for applications like environmental monitoring or smart home automation.
- Governance and Tokenization: Hedera Hashgraph's unique properties, including fairness, security, and scalability, make it a viable choice for decentralized governance systems and tokenized assets. Its robust framework ensures integrity in distributed decision-making processes.

Ultimately, the selection of a hybrid consensus mechanism should align with the specific requirements, goals, and characteristics of the intended decentralized application. By matching the mechanism to the use case, blockchain networks can achieve optimal performance, scalability, and security.

4.5. Security in Hybrid Consensus Mechanisms. Security is a critical concern in the design of hybrid consensus mechanisms, especially in the face of increasingly sophisticated attacks. While traditional surveys have explored individual vulnerabilities and defense mechanisms, they often fail to account for the interplay between consensus mechanisms and real-world network dynamics. This subsection aims to address this gap by integrating both perspectives into a comprehensive evaluation of hybrid mechanisms.

For instance, Saad et al. [97] provided an in-depth analysis of the Nakamoto consensus in asynchronous networks, yet their study does not extensively address how network-level factors, such as partitioning attacks or delays in block propagation, directly affect consensus security. Similarly, Heo et al. [2] discussed partitioning attacks in Ethereum, while Saad et al. [98] highlighted the *SyncAttack*, where double-spending can occur in Bitcoin without requiring significant mining power. These studies underscore critical vulnerabilities in traditional mechanisms but do not explore how hybrid consensus models could offer more robust defenses by combining complementary protocols.

Despite these contributions, there remains a gap in understanding how different hybrid consensus mechanisms can provide tailored security solutions against a range of attacks in diverse network settings. Specifically, the combination of PoS and BFT in hybrid mechanisms is often analyzed in isolation from the broader network behavior, leading to an incomplete understanding of their resilience in more adversarial scenarios [98].

Table 8 provides a comprehensive comparison of hybrid consensus mechanisms, evaluating their protection against key attacks and risks based on a synthesis of theoretical, experimental, and empirical studies. The ratings in Table 8 are supported by three types of evidence: theoretical analysis, experimental studies, and empirical data. Theoretical analysis includes formal proofs and analyses from the literature, while experimental studies consist of results from controlled laboratory experiments or simulations. Empirical data are derived from real-world deployments, such as Hedera's operational data. Each hybrid consensus mechanism was evaluated based on a thorough review of existing studies, with references provided in the Ref column. For instance, [77] offers theoretical and experimental evidence for Casper's security, while [98] analyzes the scalability and security of PoS + PBFT through simulations.

Table 8 highlights that while mechanisms like Hedera offer comprehensive protection across a range of risks, others, such as Microchain, provide only basic protection, emphasizing the need for tailored approaches depending on specific application requirements.

As seen in Table 8, hybrid mechanisms leverage the strengths of multiple protocols to address a range of attacks and risks. However, their effectiveness varies significantly depending on the network context and adversarial conditions. For example, Hedera demonstrates comprehensive protection, benefiting from its asynchronous Byzantine Fault Tolerance (aBFT) design and carefully balanced validator network [101], whereas PoS + PBFT mechanisms rely heavily on controlled simulations to validate security under ideal conditions [98]. In contrast, existing works like Khan et al. [13] focus on reward/punishment schemes for consensus mechanisms but fail to explore their integration into hybrid structures for evaluating overall system security.

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Table 8: Hybrid consensus mechanisms: protection against attacks and risks.

Hybrid consensus mechanism	Sybil attacks	Double-spending attacks	Byzantine faults	Unauthorized participation	Reputation manipulation	Evidence type	Ref
Casper	[+]	[++]	[++]	[+]	[+]	Theoretical; experimental	[77]
PoS + PBFT	[++]	[++]	[++]	[++]	[+]	Theoretical; controlled simulations	[98]
PBFT + PoA	[++]	[+]	[++]	[+]	[+]	Hierarchical analysis; simulation	[99]
Threshold relay + PoW	[+]	[+]	[+]	[+]	[+]	Threshold modeling; experimental	[100]
Hedera	[++]	[++]	[++]	[++]	[++]	Asynchronous BFT proof; deployed network data	[101]
HDPoA	[+]	[+]	[++]	[+]	[+]	Theoretical; field experiment	[102]
Microchain	[+]	[+]	[+]	[+]	[+]	Lightweight blockchain analysis; IoT simulations	[103]
PoL + PBFT	[++]	[+]	[++]	[++]	[+]	Cooperative consensus proof; controlled simulations	[104]

Note: []: No protection, [+]: Basic protection under limited conditions, [++]: Strong protection against most adversarial scenarios, [+++]: Comprehensive protection across diverse scenarios. Evidence is categorized as follows: theoretical (formal proofs or analysis), experimental (controlled laboratory simulations), and empirical (real-world deployment data).

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/5821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Furthermore, hybrid mechanisms are specifically designed to mitigate certain vulnerabilities, yet many existing surveys overlook the critical impact of network dynamics on consensus security. The findings in Table 8 align with insights from Saad et al. [98], who emphasize the importance of scalability and security in hybrid mechanisms under controlled conditions. However, as Tran et al. [12] suggest, these mechanisms still face challenges in addressing real-world network fluctuations.

These findings underscore the importance of considering both consensus-specific vulnerabilities and network behavior when designing hybrid mechanisms for real-world applications such as IoT and financial systems. In light of these gaps, our study makes a significant contribution by evaluating hybrid consensus mechanisms with a dual focus.

- Consensus-related vulnerabilities, such as Sybil attacks, double-spending, and long-range attacks.
- Network-level behavior, including partitioning attacks, block propagation delays, and fluctuating network conditions.

This nuanced approach provides a more comprehensive understanding of how hybrid consensus mechanisms can be tailored to secure decentralized networks under varying adversarial conditions—a consideration that has been insufficiently addressed in existing surveys.

4.5.1. Network Behavior and Consensus Mechanisms. The interaction between consensus mechanisms and underlying network behavior significantly influences the performance and security of blockchain systems. Empirical studies have demonstrated how network-level vulnerabilities, such as partitioning attacks and block propagation delays, can destabilize consensus and expose blockchain networks to adversarial attacks. For example,

Saad et al. [1, 97] provided a comprehensive analysis of the Nakamoto consensus in asynchronous networks, highlighting its vulnerabilities under network delays and partitioning.

Tran et al. [12] described a stealthier partitioning attack on Bitcoin's peer-to-peer network, revealing how subtle disruptions in communication can weaken consensus stability.

Heo et al. [2] examined partitioning attacks in Ethereum and their impact on network reliability and consensus mechanisms. Hybrid consensus mechanisms, such as PoS combined with PBFT, offer improved scalability and security by leveraging complementary strengths. However, their performance is heavily influenced by network behavior.

Saad et al. [105] introduced the SyncAttack, demonstrating how network propagation delays can enable double-spending without significant computational power.

Ahmad et al. [11] empirically compared the performance of consensus mechanisms, revealing that latency and bandwidth constraints can significantly impact hybrid models like PoS + PBFT.

Saad et al. [3] proposed e-PoS, a hybrid PoS mechanism, emphasizing the importance of decentralization and fairness in mitigating network-induced vulnerabilities. Real-world systems, such as Hedera, provide valuable insights into addressing these challenges. Hedera's aBFT design demonstrates how a carefully structured validator network can mitigate the effects of network fluctuations, ensuring resilience against adversarial conditions [101]. However, empirical studies indicate that mechanisms like PoS + PBFT, while robust in theory, require optimized synchronization protocols to address latency and bandwidth issues effectively in resource-constrained environments.

These findings underscore the importance of designing hybrid consensus mechanisms that account for network dynamics. By integrating network behavior into the evaluation of consensus mechanisms, blockchain systems can achieve enhanced stability and security, even under adversarial conditions.

4.6. Implementation of Hybrid Consensus Mechanisms. Implementing hybrid consensus mechanisms involves addressing significant technical challenges while leveraging innovative solutions. These mechanisms combine the strengths of various consensus models to optimize performance, scalability, and security in blockchain systems.

- Microchain's Deployment: Microchain's deployment on Raspberry Pi devices demonstrates lightweight blockchain solutions tailored for IoT systems [67, 68].
- Hybrid Delegated Proof of Authority and Casper: Hybrid models like Hybrid Delegated Proof of Authority and Casper showcase how integrating mechanisms such as PoS and BFT can enhance performance and security within existing blockchain architectures [62, 96].

The deployment of hybrid consensus mechanisms on platforms like Raspberry Pi presents both opportunities and limitations:

1. High-Performance Requirements: Mechanisms such as Casper and Threshold Relay with PoW often require significant computational resources, relying on specialized hardware or high-performance computing systems. This makes them less feasible for resource-constrained environments like IoT [67, 106].
2. Feasibility for IoT Devices: Hybrid mechanisms combining PoS with PBFT or PoA are more suitable for Raspberry Pi devices due to their lower computational demands. These devices can serve as validator nodes, leveraging the energy efficiency and cost-effectiveness of PoS while contributing to the consensus process [62, 106].

- Hardware Limitations: Raspberry Pi devices have constraints in processing power, memory, and network connectivity. Proper configuration and optimization are essential to ensure stability and performance in hybrid consensus networks [68, 72].

Hybrid consensus mechanisms, such as PoS with PBFT, demonstrate significant advantages in scalability and efficiency for real-world applications.

- Reduced Communication Complexity: By limiting the consensus process to a small subset of validators, mechanisms like Microchain significantly reduce

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

communication overhead, enabling efficient operation in IoT settings [62, 67].

- Improved Transaction Throughput: Faster confirmation times achieved through hybrid models make them suitable for real-time processing and IoT applications requiring quick and reliable data exchange [68, 106].

Hybrid consensus mechanisms represent a sophisticated blend of technologies designed to address traditional blockchain challenges such as scalability, energy consumption, and resource constraints. By optimizing performance and security through innovative combinations of consensus protocols, these mechanisms have the potential to revolutionize blockchain applications across IoT, finance, and real-time processing [72, 96].

5. Conclusions, Future Work, and Proposed New Hybrid Consensus Algorithm

Over recent years, blockchain technology has garnered significant attention due to its distinctive properties of decentralization, autonomy, integrity, immutability, verification capabilities, and fault tolerance. These attributes have positioned blockchain as a pivotal technology, particularly in domains that demand secure and transparent transaction mechanisms. This survey has provided an in-depth overview of hybrid consensus algorithms, which integrate elements from multiple consensus mechanisms like PoW and PoS. Despite their benefits in overcoming the limitations of singular systems, hybrid systems still face challenges related to security vulnerabilities, efficiency, and cost-effectiveness across various blockchain networks. We highlighted the application of hybrid consensus algorithms in enhancing blockchain security, ensuring identity verification, and providing nonrepudiation. These functionalities are crucial in environments where the integrity and authenticity of transactions are paramount.

5.1. Future Work. To guide future research, several key areas require focus and development as follows:

1. Addressing Security Vulnerabilities in Hybrid Consensus Systems:
   - Objective: Develop robust security measures to counteract new and evolving threats.
   - Approach: Investigate advanced cryptographic techniques, anomaly detection systems, and adaptive security protocols tailored to hybrid consensus environments.
   - Expected Outcomes: Enhanced resilience against attacks such as Sybil attacks, double-spending, and consensus manipulation, ensuring the integrity and security of blockchain networks.
2. Improving Efficiency and Cost-Effectiveness:
   - Objective: Create more efficient hybrid consensus algorithms to reduce operational costs, enhance scalability, and decrease energy consumption.
   - Approach: Explore lightweight consensus protocols, optimized resource management strategies, and energy-efficient validation processes.
   - Expected Outcomes: Reduced operational costs and energy usage, improved transaction throughput, and maintained or enhanced security and performance levels.
3. Tailoring Hybrid Consensus Mechanisms to Specific Industry Needs:
   - Objective: Adapt hybrid consensus algorithms to meet the unique requirements of various industries.
   - Approach: Conduct industry-specific case studies, develop customized consensus models, and pilot hybrid consensus systems in real-world scenarios.
   - Expected Outcomes: Increased adoption of blockchain technology in healthcare, finance, supply chain, and other sectors, leveraging the benefits of enhanced consensus mechanisms.
4. Continued Innovation and Exploration of New Applications:
   - Objective: Advance the field of hybrid consensus algorithms and unlock new use cases.
   - Approach: Encourage interdisciplinary research, foster collaboration between academia and industry, and explore novel blockchain applications.
   - Expected Outcomes: Identification of new use cases, expanded application of blockchain technology, and ongoing advancements in hybrid consensus research.

5.2. Proposed New Hybrid Consensus Algorithm. The adaptive hybrid consensus mechanism (AHCM) is a conceptual framework designed to address current challenges in blockchain scalability, security, and energy efficiency. This algorithm is part of ongoing research and aims to provide a flexible solution tailored to diverse network conditions and application requirements.

The AHCM is a conceptual framework proposed for further exploration in our ongoing research. Implementation details will be disclosed in future publications.

5.2.1. Objective. To develop a hybrid consensus mechanism capable of dynamically adapting to real-time network metrics, ensuring optimal performance and security.

5.2.2. Key Features

- Dynamic Adjustment: Switches between PoW, PoS, and other mechanisms based on transaction volume, latency, and energy consumption.
- Multilayer Security: Integrates advanced protocols such as zero-knowledge proofs and multisignature schemes.
- Industry-Specific Optimization: Allows industry-specific optimization for diverse applications.

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

5.2.3. Implementation Plan

1. Design Phase: Develop the theoretical framework and design specifications for AHCM.
2. Simulation and Testing: Use simulation tools to test the algorithm under various network conditions and scenarios.
3. Pilot Deployment: Implement pilot projects in collaboration with industry partners to validate the algorithm in real-world applications.
4. Evaluation and Iteration: Continuously evaluate performance and security, iterating on the design to address identified issues and optimize functionality.

5.2.4. Expected Outcomes

- Scalability: Enhanced scalability to handle high transaction volumes in diverse applications.
- Energy Efficiency: Reduced energy consumption through intelligent consensus mechanism switching.
- Security: Improved security through multilayer protocols and adaptive adjustments.

5.3. Summary and Outlook. Research into hybrid consensus algorithms represents a promising frontier in blockchain technology. By addressing current challenges and exploring new applications, future advancements in this area hold the potential to significantly enhance the scalability, security, and efficiency of blockchain systems, making them more adaptable and suitable for a broader range of applications.

The AHCM framework represents ongoing research by the authors. This conceptual design is intended for academic discussion, with implementation details to be shared in future works. Unauthorized use or replication is prohibited.

This survey lays the groundwork for continued innovation in the field, offering a comprehensive framework that can guide future research and development efforts.

Data Availability Statement

There are no data available for this work.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

The authors did not receive any specific grant or financial support for this research. The Article Publication Charge (APC) for this manuscript was waived by *the International Journal of Intelligent Systems*.

Acknowledgments

We would like to express our gratitude to colleagues and reviewers whose valuable feedback and constructive suggestions greatly improved the quality of this work. We also acknowledge the Deutscher Akademischer Austauschdienst (DAAD) for providing academic supervision and guidance through their program.

References

[1] M. Saad, A. Anwar, S. Ravi, and D. Mohaisen, "Revisiting Nakamoto Consensus in Asynchronous Net- Works: A Comprehensive Analysis of Bitcoin Safety and Chain Quality," *IEEE/ACM Transactions on Networking* 32, no. 1 (2024): 844–858, https://doi.org/10.1109/tnet.2023.3302955.

[2] H. Heo, S. Woo, T. Yoon, M. Kang, and S. Shin, "Partitioning Ethereum Without Eclipsing it," in *Proceedings of the 30th Annual Network and Distributed System Security Symposium (NDSS)* (The Internet Society, 2023), https://www.ndss-symposium.org/wp-content/uploads/2023/02/ndss2023_f465_paper.pdf.

[3] M. Saad, Z. Qin, K. Ren, D. Nyang, D. Mohaisen, and e-PoS, "E-PoS: Making Proof-of-Stake Decentralized and Fair," *IEEE Transactions on Parallel and Distributed Systems* 32, no. 8 (2021): 1961–1973, https://doi.org/10.1109/tpds.2020.3048853.

[4] S. Bouraga, "A Taxonomy of Blockchain Consensus Protocols: A Survey and Classification Framework," *Expert Systems With Applications* 168 (2021): 114384, https://doi.org/10.1016/j.eswa.2020.114384.

[5] Y. Elgountery, A. Boushaba, M. Oualla, and H. Sadki, "Blockchain Architecture for IoT: Comparative Survey," *The 3rd International Day on Computer Science and Applied Mathematics* 6, no. 1 (2023): 7, https://doi.org/10.3390/cmsf2023006007.

[6] 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," *Applied Sciences (Switzerland)* 13, no. 4 (2023): 2604, https://doi.org/10.3390/app13042604.

[7] V. Gugueoth, S. Safavat, S. Shetty, and D. Rawat, "A Review of IoT Security and Privacy Using Decentralized Blockchain Techniques," *Computer Science Review* 50 (2023): 100585–100616, https://doi.org/10.1016/j.cosrev.2023.100585.

[8] A. Alkhateeb, C. Catal, G. Kar, and A. Mishra, "Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review," *Sensors* 22, no. 4 (2022): 1304, https://doi.org/10.3390/s22041304.

[9] M. Šarac, N. Pavlović, S. Adamović, M. Saračević, and D. Radovanović, "Blockchain Implementation for IoT Devices: Blockchain of Things," in *Blockchain Technology Solutions for the Security of IoT-Based Healthcare Systems* (2023), 151–165.

[10] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W. C. Hong, "A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems," *IEEE Access* 8 (2020): 54371–54401, https://doi.org/10.1109/access.2020.2981415.

[11] A. Ahmad, A. Alabduljabbar, M. Saad, D. Nyang, J. Kim, and D. Mohaisen, "Empirically Comparing the Performance of Blockchain's Consensus Algorithms," *IET Blockchain* 1, no. 1 (2021): 56–64, https://doi.org/10.1049/blc2.12007.

[12] M. Tran, I. Choi, G. J. Moon, A. V. Vu, and M. S. Kang, "A Stealthier Partitioning Attack against Bitcoin Peer-To-Peer Network," in *IEEE Symposium on Security and Privacy (SP)* (2020), 894–909.

[13] M. Khan, F. den Hartog, and J. Hu, "A Survey and Ontology of Blockchain Consensus Algorithms for Resource-

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Constrained IoT Systems," *Sensors* 22, no. 21 (2022): 8188, https://doi.org/10.3390/s22218188.

[14] P. Zhang, D. C. Schmidt, J. White, G. Lenz, and S. A. Proctor, "Blockchain Technology Use Cases in Healthcare," *Advances in Computers* 121 (2018): 1–41, https://doi.org/10.1016/bs.adcom.2018.03.006.

[15] M. Salimitari, M. Chatterjee, and Y. P. Fallah, "A Survey on Consensus Methods in Blockchain for Resource-Constrained IoT Networks," *Internet of Things (Netherlands)* 11 (2020): 100212, https://doi.org/10.1016/j.iot.2020.100212.

[16] M. Salimitari and M. Chatterjee, "A Survey on Consensus Protocols in Blockchain for IoT Networks," *Ad Hoc Networks* 87 (2018): 1–15, https://doi.org/10.1016/j.adhoc.2018.09.004.

[17] P. Khobragade and A. K. Turuk, "Blockchain Consensus Algorithms: A Survey," *Lecture Notes in Networks and Systems* 595 (2023): 198–210, https://doi.org/10.1007/978-3-031-21229-1_19.

[18] G. T. Nguyen and K. Kim, "A Survey about Consensus Algorithms Used in Blockchain," *Journal of Information Processing Systems* 14, no. 1 (2018): 101–128.

[19] A. M. Alqahtani and A. Algarni, "A Survey on Blockchain Technology Concepts, Applications and Security," *International Journal of Advanced Computer Science and Applications* 14, no. 2 (2023): 841–847, https://doi.org/10.14569/ijacsa.2023.0140296.

[20] A. Dahiya, B. B. Gupta, W. Alhalabi, and K. Ulrichd, "A Comprehensive Analysis of Blockchain and its Applications in Intelligent Systems Based on IoT, Cloud and Social Media," *International Journal of Intelligent Systems* 37, no. 12 (2022): 11037–11077, https://doi.org/10.1002/int.23032.

[21] M. G. Gedam and S. Karmore, "Blockchain-Based IoT: A Comprehensive Review of Technology Integration, Security, and Scalability," in *Proceedings of the Conference on Advances in Computing and Communication* (2024), 395–406, https://doi.org/10.1007/978-981-97-0180-3_31.

[22] G. Tripathi, M. A. Ahad, and G. Casalino, "A Comprehensive Review of Blockchain Technology: Underlying Principles and Historical Background With Future Challenges," *Decision Analytics Journal* 9 (2023): 100344, https://doi.org/10.1016/j.dajour.2023.100344.

[23] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain Consensus Algorithms: A Survey," *IEEE Access* 8 (2020): 48798–48822.

[24] S. Pahlajani, A. Kshirsagar, and V. Pachghare, "Survey on Private Blockchain Consensus Algorithms," *International Journal of Computer Applications* 176, no. 29 (2020): 15–23.

[25] S. J. Alsunaidi and F. A. Alhaidari, "A Survey of Consensus Algorithms for Blockchain Technology," *International Journal of Blockchain and Distributed Ledger Technology* 3 (2022): 12–27.

[26] M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, "A Survey of Consensus Algorithms in Public Blockchain Systems for Cryptocurrencies," *Springer Lecture Notes in Computer Science* 12848 (2022): 312–329.

[27] K. Sharma, D. Jain, A. Kshirsagar, and V. Pachghare, "Consensus Algorithms in Blockchain Technology: A Survey," *International Journal of Information Security and Privacy* 15, no. 2 (2021): 15–28.

[28] V. Buterin, *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform* (Ethereum Foundation, 2013).

[29] S. Nakamoto, in *Bitcoin: A Peer-To-Peer Electronic Cash System*, https://www.bitcoin.org.

[30] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, and J. Clark, *Bitcoin and Cryptocurrency Technologies: Introduction to the Book* (2016).

[31] S. Zhou, K. Li, L. Xiao, J. Cai, W. Liang, and A. Castiglione, "A Systematic Review of Consensus Mechanisms in Blockchain," *Mathematics* 11, no. 10 (2023): 2248–2327, https://doi.org/10.3390/math11102248.

[32] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges," *IEEE Access* 8 (2020): 32031–32053, https://doi.org/10.1109/access.2020.2973178.

[33] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A Survey of Blockchain Consensus Algorithms Performance Evaluation Criteria," *Expert Systems With Applications* 154 (2023): 113385.

[34] J. Bou Abdo, R. El Sibai, and J. Demerjian, "Permissionless Proof-of-Reputation-X: A Hybrid Reputation-Based Consensus Algorithm for Permissionless Blockchains," *Transactions on Emerging Telecommunications Technologies* 32, no. 1 (2021): e4148, https://doi.org/10.1002/ett.4148.

[35] S. Joshi, in *Feasibility of Proof of Authority as a Consensus Protocol Model* (2021).

[36] B. Sriman, S. Ganesh Kumar, and P. Shamili, "Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake," in *Advances in Intelligent Systems and Computing*, 1172 (Springer, 2021), 395–406, https://doi.org/10.1007/978-981-15-5566-4_34.

[37] C. Natoli and V. Gramoli, "The Balance Attack or Why Forkable Blockchains Are Ill-Suited for Consortium," in *Proceedings-47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2017* (IEEE, 2017), 579–590.

[38] Y. Wu, P. Song, and F. Wang, "Hybrid Consensus Algorithm Optimization: A Mathematical Method Based on POS and PBFT and its Application in Blockchain," *Mathematical Problems in Engineering 2020* (2020): 7270624.

[39] M. Andoni, V. Robu, D. Flynn, et al., "Blockchain Technology in the Energy Sector: A Systematic Review of Challenges and Opportunities," *Renewable and Sustainable Energy Reviews* 100 (2019): 143–174, https://doi.org/10.1016/j.rser.2018.10.014.

[40] S. Micali, in *Algorand: The Efficient and Democratic Ledger* (2016).

[41] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," *OSDI* 99 (1999): 173–186.

[42] E. Buchman, *Tendermint: Byzantine Fault Tolerance in the Age of Blockchains* (University of Guelph, 2018), https://tendermint.com/static/docs/tendermint.pdfPhD Thesis.

[43] M. Westerkamp and M. Diez, "Verilay: A Verifiable Proof of Stake Chain Relay," in *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2022* (IEEE, 2022), 7–10.

[44] R. Zhang and B. Preneel, in *Towards a Fully Decentralized Cross-Blockchain Transfer Protocol* (2020).

[45] P. Kochovski and V. Stankovski, "Interledger Protocol for Blockchain Interoperability," *IEEE Transactions on Cloud Computing* 9, no. 3 (2021): 759–771.

[46] Y. Li, C. Chen, N. Liu, H. Huang, Z. Zheng, and Q. Yan, in *Verilay: A Verifiable Proof of Stake Chain Relay* (2020).

[47] H. Wang, B. Chen, and J. Zhang, "Performance Analysis of Blockchain-Based Systems: Current Status and Future Perspectives," *Journal of Network and Computer Applications* 136 (2019): 85–94.

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

[48] K. Qin, L. Zhou, and B. Livshits, in *Attacking the DeFi Ecosystem With Flash Loans for Fun and Profit* (2021).
[49] S. Werner, D. Perez, and B. Livshits, in *SoK: Decentralized Finance (DeFi)* (2021).
[50] I. Makarov and A. Schoar, "Cryptocurrencies and Decentralized Finance," *The Journal of Economic Perspectives* 36, no. 4 (2022): 91–114, https://ssrn.com/abstract=4104550.
[51] H. Ali and S. Saleem, in *Non-Fungible Tokens (NFTs): Applications and Challenges* (2021).
[52] H. Zhang, Y. Zhang, and T. Taleb, "Blockchain and Multi-Access Edge Computing: Emerging Trends and Challenges," *IEEE Communications Magazine* 58, no. 3 (2020): 20–26.
[53] M. Kim, J. Seo, M. Aslam, W. Na, and S. Kim, "Blockchain-Based Data Provenance for IoT Applications in Smart Home Environments," in *Proceedings of the IEEE Conference on Blockchain* (2018), 1350–1355.
[54] L. Baird, M. Harmon, and P. Reitz, "Hedera Hashgraph: Applications and Performance in the Real World," *IEEE Blockchain* (2019): https://hedera.com.
[55] A. Garg and I. Pahwa, "Performance and Scalability Analysis of Blockchain Consensus Mechanisms," *Journal of Emerging Technologies* 9 (2020): 123–134.
[56] M. Wang and Q. Zhang, "Hashgraph vs Blockchain: A Comprehensive Analysis of Consensus Algorithms," *Journal of Distributed Ledger Technology* 4, no. 1 (2020): 1–12.
[57] K. Xu and H. Yang, "Blockchain-Based MEC Networks: Enhancing Security and Scalability," *IEEE Access* 9 (2021): 16520–16532.
[58] P. Sharma and R. Kumar, "Integration of MEC and Blockchain for Secure and Scalable IoT Applications," in *Proceedings of the 2020 International Conference on Internet of Things (IoT) ACM* (2020), 56–61.
[59] Y. Tang, J. Yan, C. Chakraborty, and Y. Sun, "Hedera: A Permissionless and Scalable Hybrid Blockchain Consensus Algorithm in Multi-Access Edge Computing for IoT," *IEEE Internet of Things Journal* (2023): 1.
[60] S. Alrubei, E. Ball, and J. Rigelsford, "Honesty-Based Distributed Proof of Authority: Honesty-Based Distributed Proof of Authority via Scalable Work Consensus Protocol for IoT-Blockchain Applications," *Computer Networks* 217 (2022): 109337–109410, https://doi.org/10.1016/j.comnet.2022.109337.
[61] J. Zhang, B. Chen, and L. Xu, "Blockchain for IoT: An Energy-Efficient Consensus Algorithm for Resource-Constrained Devices," *IEEE Internet of Things Journal* 8, no. 5 (2021): 3602–3615.
[62] Y. Wang, J. Liu, and H. Zhang, "Combining Proof-of-Work and Proof-of-Authority for Scalable and Secure IoT Blockchain Applications," *Future Generation Computer Systems* 100 (2019): 345–356.
[63] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (2017): 618–623, https://doi.org/10.1109/percomw.2017.7917634.
[64] L. Gao, T. Xu, and X. Zhang, "Security and Privacy Challenges in IoT: Blockchain-Based Solutions," *IEEE Communications Surveys & Tutorials* 22, no. 2 (2020): 1046–1073.
[65] M. Ali, A. H. Fahad, and A. Saleem, "Secure Blockchain-Based Framework for IoT Data Integrity and Efficiency," *Sensors* 21, no. 5 (2021): 1652.
[66] W. Xu, Y. Zhang, and X. Lin, "Efficient Blockchain Consensus for IoT Networks: A Comparative Study," *Journal of Network and Computer Applications* 159 (2020): 102598.
[67] B. Zhang, T. Li, and H. Wang, "Lightweight Blockchain Protocols for Secure IoT Systems: A Survey," *Computers & Security* 110 (2021): 102470.
[68] X. Xu, I. Weber, and M. Staples, *Data Quality Challenges in Blockchain. Blockchain: Technologies and Applications for Industry 40* (2019).
[69] Q. Wang and T. Lee, "Verifiable Random Function (VRF) Based Committee Selection for Lightweight IoT Consensus," *IEEE Transactions on Network and Service Management* 17, no. 4 (2020): 2524–2536.
[70] S. Mukherjee and S. Biswas, "Blockchain for IoT: A Survey on Lightweight Consensus Mechanisms," *IEEE Access* 9 (2021): 103422–103441.
[71] L. Gao, J. Xu, and X. Zhang, "A Lightweight and Secure Blockchain Framework for IoT-Based Applications," *Journal of Network and Computer Applications* 182 (2021): 102828.
[72] Z. Auhl, N. Chilamkurti, R. Alhadad, and W. Heyne, "A Comparative Study of Consensus Mechanisms in Blockchain for IoT Networks," *Electronics* 11, no. 17 (2022): 2694, https://doi.org/10.3390/electronics11172694.
[73] S. Tanwar, "Consensus Scalability in Blockchain Network," in *Blockchain Technology: From Theory to Practice* (Springer, 2022), 251–272.
[74] R. Kumar, J. Lachure, and R. Doriya, "Hybrid Consensus Approach for Blockchain Based Vehicular Communication," in *2022 Second International Conference on Power, Control and Computing Technologies (ICPC2T)* (IEEE, 2022), 1–6.
[75] D. S. K. Putra and A. Amiruddin, "A Proposed Architecture for the Indonesia's National Blockchain," in *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)* (2023), 230–235, https://doi.org/10.1109/icocics58778.2023.10277291.
[76] S. Popov, O. Moog, and A. Camargo, "The IOTA Consensus Mechanism: Exploring DAG and Proof of Stake for IoT Networks," *Journal of Blockchain Technology* 5, no. 2 (2023): 45–60, https://iota.org/research/consensus-dag-pos.
[77] V. Buterin and V. Griffith, in *Casper the Friendly Finality Gadget* (2017).
[78] E. Buchman, "Tendermint: Byzantine Fault Tolerance in the Age of Blockchains," in *Master's Thesis* (University of Guelph, 2016), https://tendermint.com/static/docs/tendermint.pdf.
[79] S. Popov, in *The Tangle* (2017), https://arxiv.org/abs/1702.05725.
[80] E. Androulaki, A. Barger, V. Bortnikov, et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proceedings of the 13th EuroSys Conference* (2018), 1–15, https://dl.acm.org/doi/10.1145/3190508.3190538.
[81] X. Xu, Y. Jin, Z. Zeng, S. Yang, and R. Chen, "Hierarchical Lightweight High-Throughput Blockchain for Industrial Internet Data Security, Computer Integrated Manufacturing Systems," *Computer Integrated Manufacturing System* 25, no. 12 (2019): 3258–3266.
[82] H. Hou and Z. Cao, "Vechain Blockchain Technology for Supply Chain Management," *Future Internet* 10, no. 8 (2018): 106.
[83] A. Dorri and R. Jurdak, "Tree-Chain: A Fast Lightweight Consensus Algorithm for IoT Applications," in *2020 IEEE 45th Conference on Local Computer Networks (LCN)* (2020), 369–372, https://doi.org/10.1109/lcn48667.2020.9314831.

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

[84] M. Uddin, M. Muzammal, M. K. Hameed, I. T. Javed, B. Alamri, and N. Crespi, "CBCIoT: A Consensus Algorithm for Blockchain-Based IoT Applications," *Applied Sciences (Switzerland)* 11, no. 22 (2021): 11011, https://doi.org/10.3390/app112211011.

[85] P. Prabha and K. Chatterjee, "Design and Implementation of Hybrid Consensus Mechanism for IoT Based Healthcare System Security," *International Journal on Information Technology* 14, no. 3 (2022): 1381–1396, https://doi.org/10.1007/s41870-022-00880-6.

[86] B. Wang, Z. Li, and H. Li, "Hybrid Consensus Algorithm Based on Modified Proof-of-Probability and DPoS," *Future Internet* 12, no. 8 (2020): 122–216, https://doi.org/10.3390/fi12080122.

[87] Y. Song, G. Fan, Y. Long, Z. Liu, X. Xu, and D. Gu, "Grape: Efficient Hybrid Consensus Protocol Using DAG," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 13619 (LNCS Springer International Publishing, 2023), 258–274, https://doi.org/10.1007/978-3-031-25734-6_16.

[88] C. Sun, D. Li, B. Wang, and J. Song, "AI-Enabled Consensus Algorithm in Human-Centric Collaborative Computing for Internet of Vehicle," *Symmetry* 15, no. 6 (2023): 1264, https://doi.org/10.3390/sym15061264.

[89] H. Zhang, Y. Li, and Y. Zheng, "Consensus of Second-Order Heterogeneous Hybrid Multiagent Systems via Event-Triggered Protocols," *Complexity* 2022, no. 1 (2022): https://doi.org/10.1155/2022/2665925.

[90] 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* 13, no. 11 (2021): 285, https://doi.org/10.3390/fi13110285.

[91] Z. Cheng, G. Wu, H. Wu, M. Zhao, L. Zhao, and Q. Cai, in *A New Hybrid Consensus Protocol: Deterministic Proof of Work* (2018).

[92] C. X. Zhou, Q. S. Hua, and H. Jin, "HotDAG: Hybrid Consensus via Sharding in the Permissionless Model," in *Wireless Algorithms, Systems, and Applications: 15th International Conference, WASA 2020, Qingdao, China, September 13–15, 2020, Proceedings, Part I 15* (Springer, 2020), 807–821.

[93] Z. Ding, X. Dong, J. Shen, and Z. Cao, "A Hybrid Double-Layer BFT Consensus Protocol for Large-Scale IoT Blockchain," in *2022 2nd International Conference on Frontiers of Electronics, Information and Computation Technologies (ICFEICT)* (2022), 354–361, https://doi.org/10.1109/icfeict57213.2022.00071.

[94] Y. Pan, W. Wei, Y. Liu, and C. Zhu, "Hybrid Consensus Algorithm Based on Hierarchy Authority," in *2021 IEEE International Conference on Electronic Technology, Communication and Information (ICETCI)* (2021), 553–559, https://doi.org/10.1109/icetci53161.2021.9563559.

[95] Y. Liu, T. Tan, and Y. Zhuo, "Hybrid Consensus Protocols and Security Analysis for Blockchain," in *2022 International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI)* (IEEE, 2022), 191–195.

[96] L. Baird, *The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerant* (Swirlds Whitepaper, 2016), https://www.swirlds.com/whitepapers.

[97] M. Saad, A. Anwar, S. Ravi, and D. Mohaisen, "Revisiting Nakamoto Consensus in Asynchronous Networks: A Comprehensive Analysis of Bitcoin Safety and Chain Quality," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (2021), 988–1005, https://doi.org/10.1145/3460120.3484561.

[98] M. Saad, J. Spaulding, L. Njilla, et al., "Exploring the Attack Surface of Blockchain: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials* 22, no. 3 (2020): 1977–2008, https://doi.org/10.1109/comst.2020.2975999.

[99] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain," in *Proceedings of Italian Conference on Cyber Security (ITASEC)* (Milan, Italy, 2018), 11.

[100] S. Bano, A. Sonnino, M. Al-Bassam, et al., in *SoK: Consensus in the Age of Blockchains* (2017).

[101] L. Baird, "The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance," *Swirlds Tech Report* (2016).

[102] A. Kumar Jha, "Hybrid Consensus Mechanism (HCM): Achieving Efficient and Secure Consensus in Blockchain," *SSRN Electronic Journal* (2023): https://doi.org/10.2139/ssrn.4413290.

[103] M. Li, X. Luo, K. Xue, Y. Xue, W. Sun, and J. Li, "A Secure and Efficient Blockchain Sharding Scheme via Hybrid Consensus," *IEEE Transactions on Information Forensics and Security* 19 (2024): 5911–5924, https://doi.org/10.1109/TIFS.2024.10539974.

[104] M. Ipchi Sheshgelani, S. Pashazadeh, and P. Salehpoor, "Cooperative Hybrid Consensus With Function Optimization for Blockchain," *Cluster Computing* 26, no. 6 (2023): 3565–3576, https://doi.org/10.1007/s10586-022-03746-5.

[105] M. Saad, S. Chen, and D. Mohaisen, "SyncAttack: Double-Spending in Bitcoin Without Mining Power," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (2021), 1668–1685, https://doi.org/10.1145/3460120.3484568.

[106] Y. Liu, W. Zhao, and Q. Zhang, "Secure and Efficient Blockchain-Based IoT Framework Using Consensus Mechanism," *Sensors* 20, no. 6 (2020): 1728.

ijis, 2025, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1155/int/3821997 by Hochschule Offenburg, Wiley Online Library on [13/05/2025]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License