Hybrid Consensus Architectures for Blockchain-Enabled IoT Systems: Challenges, Solutions, and Future Directions

[1,2]**Dr. N. A. Natraj, [3]Dr. Midhunchakkaravarthy, J. J., [4]Dr. Brojo Kishore Mishra, [5]Ms. Supriya Shrikant Laykar**

[1,5]Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University), Pune, Maharashtra, India

[2]Post-Doctoral Research Fellow, Lincoln University College, Selangor, Malaysia

[3]Faculty of AI Computing and Multimedia, Lincoln University College, Selangor, Malaysia

[4]Department of Computer Science and Engineering, NIST University, Berhampur, Orissa, India

[5]Dr.D.Y.Patil Prathisthan's College of Engineering, Kolhapur, Maharashtra, India

natraj@sidtm.edu.in, pdf.natraj@lincoln.edu.my, midhun@lincoln.edu.my, brojokishoremishra@gmail.com, supriyalaykar7@gmail.com

Corresponding author: **N. A. Natraj (**natraj@sidtm.edu.in, pdf.natraj@lincoln.edu.my)

Abstract: The application of blockchain technology to IoT systems offers substantial potential for enhancing the security of critical systems by addressing data integrity issues in increasingly susceptible network environments. Traditional blockchain consensus methods exhibit significant limitations when applied in IoT frameworks, as they do not adequately address resource constraints or operational requirements. This study investigates the integration of various consensus models within hybrid consensus solutions to effectively address IoT requirements through the optimization of performance parameters. This paper introduces a systematic framework for analyzing diverse methodologies, including combinations of Proof of Work (PoW) and Proof of Stake (PoS), PBFT enhanced with PoW/PoS components, hierarchical solutions for multi-tier IoT systems, reputation-based models, and time-sensitive frameworks. Three case studies—namely IOTA's Tangle, IoTeX's Roll-DPoS, and Hyperledger Fabric—illustrate practical applications within the healthcare and industrial automation sectors. The performance assessment framework identifies significant trade-offs among scalability, energy efficiency, transaction throughput, security guarantees, fault tolerance, and latency. This study analyzes implementation challenges such as standardization issues, security vulnerabilities, scalability limitations, integration complexities with edge-fog computing, and regulatory requirements. Progress in this field necessitates the establishment of standardized interoperability frameworks, the development of improved security evaluation methodologies, the creation of solutions for ultra-scale networks, and the implementation of regulatory-compliant designs. Our findings suggest that well-structured hybrid consensus mechanisms provide effective solutions for the integration of blockchain in IoT applications.

Keywords: Blockchain Technology, Internet of Things (IoT), Hybrid Consensus Mechanisms, Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Hierarchical Consensus, Reputation-based Systems, Scalability, Energy Efficiency, Security, Directed Acyclic Graph (DAG), IoT Security, Distributed Ledger Technology

1. Introduction

The Internet of Things experienced significant growth as the usage of connected devices and network bandwidth increased globally (Pal et al., 2020). The significant rise in IoT technologies introduces new security vulnerabilities due to the critical information generated by these systems (Pal et al., 2020). Various operational and security measures are implemented in IoT systems to ensure data integrity, privacy preservation, hardware integrity, and network security (Dirin et al., 2023). The interconnected operational features of IoT systems, coupled with their extensive management of sensitive data, including

personal financial and healthcare information (Dirin et al., 2023), necessitate these standards. Insufficient security features in IoT systems result in detrimental consequences that go beyond mere data leakage. Unsecured areas in IoT systems lead to significant economic losses and a reduction in user trust in these platforms. Regular system maintenance is essential to prevent equipment failures arising from the security risks associated with connected systems (Dirin et al., 2023). IoT statistics play a vital role in sophisticated applications that utilize industrial IoT and AI technologies (Zorrilla & Yebenes, 2022). Blockchain technology serves as an innovative solution that effectively addresses critical security and data integrity challenges within IoT ecosystems (Verma et al, 2024). The blockchain security framework offers decentralization, ensuring tamper resistance and transparency, which enhances IoT protection and fosters trust among connected devices and users (Sulaeman, 2025). The fundamental characteristics of blockchain—immutable records, decentralized operation, and cryptographic security—enhance the security of IoT networks by safeguarding data and ensuring authenticated communications between devices (Parmar & Kaur, 2021). The technology establishes permanent, traceable records of device connections, ensuring complete data authenticity and trackability for each component within the IoT network (Oh, 2025). Blockchain platforms facilitate smart contracts that automate security protocols, providing authorized access to IoT data and enhancing privacy protection, as noted by Oh (2025). The foundational infrastructure established by blockchain enables businesses to develop trustworthy decentralized operational models while safeguarding the IoT environment (Almarri & Aljughaiman, 2024). The conventional blockchain consensus mechanisms that have proven effective in other contexts do not meet the stringent operational requirements of IoT systems, according to Kim and Kim (2023). The application of Proof of Work (PoW) and Proof of Stake (PoS) consensus mechanisms presents challenges for IoT devices due to their high computational requirements and energy consumption, which exceed the hardware capabilities of these devices (Vavilis et al., 2025). Proof of Work mining necessitates significant energy consumption, particularly when executed on battery-powered devices with constrained processing capabilities (Vavilis et al., 2025). The enhanced energy efficiency of Proof of Stake (PoS) systems compared to Proof of Work (PoW) presents significant challenges for large-scale deployments of IoT networks (IBM, 2021a). The scalability of a large IoT network renders Practical Byzantine Fault Tolerance (PBFT) ineffective due to increasing communication complexities associated with network expansion (Zhuang et al., 2024). The resource limitations of IoT devices establish a significant gap with conventional blockchain consensus mechanisms such as PoW and PoS, thereby requiring targeted and efficient solutions tailored for IoT, as noted by Khan et al. (2022).

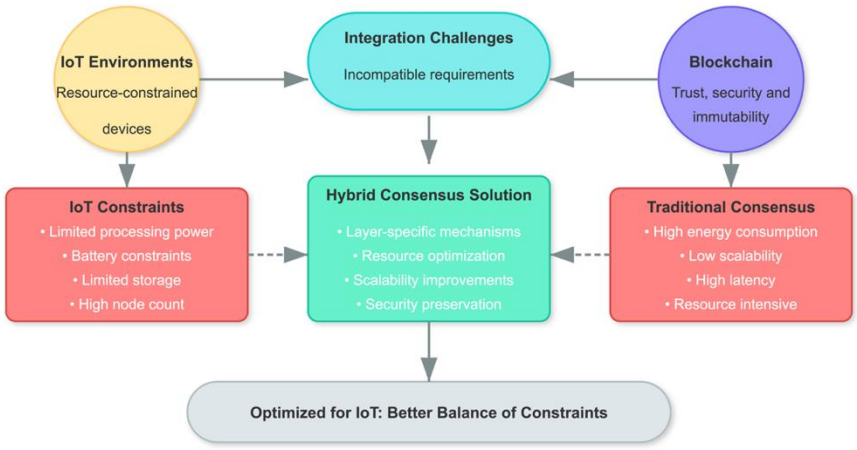

Figure 1: Conceptual overview of IoT-blockchain integration challenges and the hybrid consensus solution approach

Integrating blockchain with IoT necessitates significant adjustments due to substantial discrepancies between the capabilities of IoT devices and the requirements of blockchain, as illustrated in Figure 1. Many IoT devices function with constrained computational capacity, limited battery life, and restricted memory availability. Conventional blockchain consensus methods require significant computational power, substantial energy consumption, and ongoing communication bandwidth. Hybrid consensus mechanisms integrate various consensus types into a unified system, optimizing security efficiency by balancing scalability, energy utilization, and transaction speed. Hybrid consensus solutions in the IoT technological sector effectively address specific IoT requirements (Zhuang et al., 2024). These models identify optimal configurations for blockchain performance factors, including security, energy consumption, network scalability, and transaction speed, to ensure effective implementation of IoT blockchain (de Morais et al., 2023). Combinations of multi-consensus algorithms create hybrid mechanisms that produce robust solutions, addressing specific weaknesses in diverse IoT applications (de Morais et al., 2023). The study indicates that conventional consensus methods by themselves are insufficient to address the diverse management challenges present in various Internet of Things systems (Alkhateeb et al., 2022).

This research paper comprises eight structured sections that analyze hybrid consensus mechanisms for the application of blockchain in IoT contexts. The study commences with an introduction that explores the security challenges of IoT and discusses blockchain solutions, while highlighting the shortcomings of traditional consensus methods for IoT devices. The second section elucidates fundamental concepts of blockchain technology, the mechanics of consensus, and the unique characteristics of IoT environments, while also addressing the challenges associated with integrating these technologies. The third section examines the issues associated with prevalent consensus methods such as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), and Directed Acyclic Graph (DAG) systems in the context of Internet of Things (IoT) configurations. The fourth section constitutes the primary focus of the study, analyzing various hybrid models that integrate different consensus approaches to address existing limitations. This research examines combinations of Proof of Work (PoW) and Proof of Stake (PoS), modified Practical Byzantine Fault Tolerance (PBFT) systems, multi-level hierarchical methods, reputation-based mechanisms, and solutions for time-sensitive applications. The fifth section elucidates the examination of real-world examples such as IOTA's Tangle, IoTeX's Roll-DPoS, and Hyperledger Fabric to comprehend the practical application of these hybrid approaches. The sixth section analyzes the performance of various hybrid methods based on critical factors such as energy consumption, scalability, transaction speed, security features, fault management, and response time. Section seven addresses unresolved challenges and proposes future research directions, including the necessity for common standards, security issues, scaling difficulties, and regulatory concerns. The final section summarizes key findings and concludes that hybrid consensus methods demonstrate potential for blockchain-IoT integration; however, significant work remains before widespread implementation can occur.

2. Background and Foundational Concepts

Blockchain technology is characterized by distributed transaction monitoring via a peer-to-peer network, eliminating the necessity for centralized governing bodies (Wingreen et al., 2020). This system organizes data in blocks that are interconnected via cryptographic techniques, forming an immutable chain that safeguards against tampering and guarantees data integrity (Tanwar, 2018). Blockchains employ decentralization to distribute control among network participants, immutability to safeguard against modifications of recorded transactions, and consensus as the mechanism for collective verification of transactions within the network (Tanwar, 2018). The blockchain structure consists of blocks that include transaction data, timestamps indicating when blocks are added, and cryptographic hashes linking to preceding blocks (Black Duck, n.d.). Blockchain networks are categorized into two primary types:

permissioned networks, which are restricted to designated known entities, and permissionless networks, which permit unrestricted participation (Jaradat et al., 2021). Blockchain platforms facilitate the deployment and execution of smart contracts, which are automated agreements encoded directly into the blockchain protocol (Jaradat et al., 2021). The fundamental principles of decentralization, consensus, and immutability establish a robust framework for tackling security and trust challenges in IoT distributed systems (Tanwar, 2018).

Consensus mechanisms function to uphold agreement within blockchain networks regarding their current state (Almarri & Aljughaiman, 2024). The primary objective is to validate and prevent fraud by implementing established transaction recording rules for participant consent, thereby ensuring data coherence and operational integrity within the system (Yuan et al., 2025). Diverse development has led to the creation of multiple consensus methods, necessitating critical compromises among security, speed, scalability, and energy efficiency (Lepore et al., 2020). Blockchain consensus mechanisms include computationally intensive Proof of Work (PoW), Stake-based Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerant (PBFT), Proof of Authority (PoA), and Directed Acyclic Graph (DAG)-based alternatives (Nguyen et al., 2019). Hybrid consensus mechanisms emerged as researchers sought to improve various mechanisms by integrating them with traditional consensus strategies (Aggarwal & Kumar, 2021). The performance and security of blockchain networks are significantly influenced by the appropriate choice of consensus mechanisms, with IoT-specific requirements being essential factors in this decision (Ahakonye et al., 2024).

IoT environments are characterized by a vast number of connected devices, ranging from thousands to millions, which possess limited processing power, storage capacity, and energy resources (Khan et al., 2022). The extensive data generation in these contexts necessitates blockchain solutions that function with high speed and minimal latency for the real-time processing of IoT data required by various applications, as noted by Ragul et al. (2025). Heterogeneity issues in IoT ecosystems arise from the diverse manufacturers that produce devices using multiple communication protocols, leading to significant interoperability challenges (Zhuang et al., 2024). Security is paramount in IoT systems due to the necessity of protecting sensitive data from breaches and safeguarding controlled infrastructure against physical threats (Pal et al., 2020). The unique features of IoT environments necessitate blockchain solutions to address limitations identified in early cryptocurrency applications, as resource constraints and real-time requirements are less critical in that context (Ragul et al., 2025).

The application of blockchain technology in IoT encounters several fundamental challenges within this specialized context. Scalability presents a significant challenge as conventional blockchain networks are inadequate for handling the vast number of IoT devices and the substantial data they generate (Sulaeman, 2025). The power demands of conventional consensus mechanisms pose significant challenges for IoT devices that rely on battery power and require extended periods of operation without recharging (Sulaeman, 2025). The limited computing capabilities of most IoT devices hinder the implementation of blockchain protocols designed for advanced systems (Sulaeman, 2025). The integration necessitates a solution to achieve seamless interoperability between various IoT devices and blockchain platforms (Oh, 2025). Comprehensive testing and verification procedures are essential for smart contracts governing blockchain automation in IoT, as their security vulnerabilities pose significant risks to system integrity (Eze et al., 2019). The implementation of decentralized public blockchains in IoT systems requires addressing regulatory ambiguities and ensuring compliance with GDPR privacy standards, as these elements influence data immutability (Makhdoom et al., 2019). This technical cooperation necessitates innovation to create tailored consensus mechanisms for the effective implementation of blockchain within IoT systems, as outlined by Obaidat et al. (2024).

3. Limitations of Traditional Consensus Mechanisms in IoT Environments

Implementation of Proof of Work (PoW) in IoT systems presents significant challenges, as noted by Hsueh & Chin (2023). The high energy consumption inherent in the proof-of-work algorithm, stemming from its need for complex cryptographic puzzle solving, poses challenges for battery-powered IoT devices with constrained resources. Proof of Work poses significant implementation challenges for IoT devices due to their limited computational processing capabilities and the requirement for specialized hardware (Ragul et al., 2025). The limited transaction speed and prolonged confirmation times associated with Proof of Work fail to meet the immediate data processing needs commonly encountered in Internet of Things applications that require rapid and dependable data validation (Hsueh & Chin, 2023). IoT applications are susceptible to security vulnerabilities stemming from 51% attacks, which occur when a single entity achieves control over the hash power in proof-of-work networks (Amin, 2020). The fundamental design principle of Proof-of-Work relies on extensive computations; however, it conflicts with the computational and power limitations inherent in IoT devices, rendering it unsuitable for widespread implementation in IoT systems (Ragul et al., 2025). Figure 2 illustrates the resource requirements of consensus mechanisms.

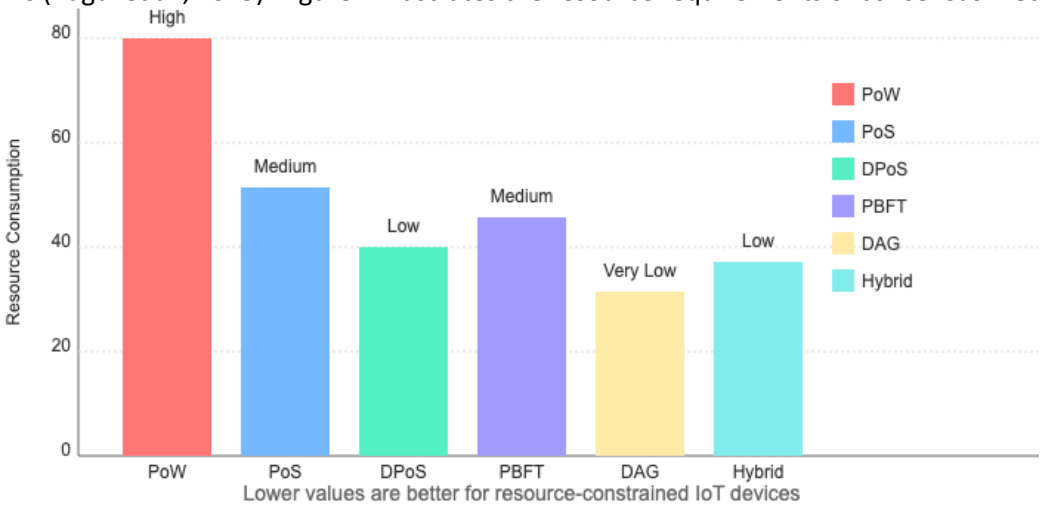

Figure 2. Resource Requirements of Consensus Mechanisms

Proof of Stake (PoS) functions as an alternative consensus mechanism that demonstrates greater energy efficiency relative to Proof of Work (PoW), while also presenting significant challenges for Internet of Things (IoT) environments. The network encounters a significant challenge as validators are selected more frequently based on their substantial stakes and contributions. Zhuang et al. (2024). According to Nguyen et al. (2019), the centralization of network control by resource-rich entities poses a risk to the decentralized nature of IoT environments. The "nothing at stake" vulnerability leads to validators casting conflicting votes on blockchain history without facing penalties, resulting in network forks that compromise IoT application security and erode customer trust (Ramírez-Gordillo et al., 2025). The long-range attack vulnerability enables an attacker to create a historical fork by gradually amassing adequate stake over time, as noted by Lepore et al. (2020). Proof of Stake systems, while more resource-efficient than Proof of Work, necessitate a thorough examination of resource consumption limits, particularly given the connectivity demands of various IoT device types (Ragul et al., 2025). The introduction of IoT network token distribution patterns represents a second factor that may lead to unbalanced outcomes for stakeholders involved in the staking process (Lepore et al., 2020).

The DPoS mechanism allows users to select a limited number of delegates responsible for approving transactions on the platform, thereby aiming to improve scalability (Ragul et al., 2025). This method accelerates the authentication process, resulting in increased transaction volume that aligns with advancements in IoT. Ragul et al. assert that diminished decentralization results from enhanced network

performance in DPoS, as the representatives chosen in the delegate selection process assume responsibility for network security and reliability. 2025. The primary risks to trust within the IoT ecosystem include the potential for collusion and the compromise of any chosen delegates. The efficacy of DPoS IoT is contingent upon the participation of token holders in the voting process, alongside the appropriate selection of representatives and their commitment to integrity standards. The integrity and utility of the IoT blockchain may decline if voters fail to participate in the process or if unrefined delegates are chosen. In comparison to Proof of Work (PoW) and certain variants of Proof of Stake (PoS), the resource requirements for implementing Delegated Proof of Stake (DPoS) are significantly lower; however, the constraints of Internet of Things (IoT) hardware must be considered prior to solution deployment (Sapra et al., 2023).

Gupta et al. present the Practical Byzantine Fault Tolerance (PBFT) system, which is a leader-based and consensus-driven algorithm that facilitates consensus in blockchain networks, even when up to one-third of its nodes are malicious or faulty. 2019.The robust fault-tolerance capability of PBFT is crucial for ensuring the reliability of IoT systems through the maintenance of accurate and consistent data processing. PBFT provides rapid transaction finality, enabling efficient data verification in applications requiring prompt command and data validation (Qi & Guan, 2023). In the domain of IoT, PBFT exhibits a significant drawback due to its high communication costs, which increase quadratically with the total number of participants (Zhuang et al., 2024). The significant scalability constraints of PBFT render it unsuitable for the management of large IoT networks, which typically comprise numerous IoT devices (Haque et al., 2024). The performance and security of PBFT are significantly influenced by the leader (primary) node, as system vulnerabilities emerge when this node is compromised or subjected to an attack (Qi & Guan, 2023). Failure points in leader election present security vulnerabilities that jeopardize network systems (Liu et al., 2023). Gupta et al. (2019) indicate that PBFT performs optimally in permissioned networks characterized by known participants and a limited number of nodes. The application of PBFT in permissionless IoT environments faces challenges due to the difficulty in managing numerous and variable nodes, alongside the protocol's susceptibility to Sybil attacks (Liu et al., 2023).

DAG-based systems present a novel alternative to traditional blockchains, offering significant advantages for IoT applications. DAG structures facilitate high parallel processing and enhanced transaction speed by enabling the simultaneous detection of multiple transaction paths, rather than depending on linear processing (Qu et al., 2024). The parallel processing model renders this system highly suitable for the extensive data processing demands of IoT devices. DAG-based systems process transaction confirmations more rapidly than traditional blockchains, making them suitable for IoT applications that require timely data validation (Raikwar et al., 2024). The absence of transaction fees in Tangle and other DAG-based platforms renders them suitable for IoT applications that depend significantly on microtransactions, as noted by Sealey et al., 2022. DAG-based protocols employ diverse methods for transaction validation and ordering within their framework; however, attaining robust consensus and security remains a complex challenge (Uddin et al., 2021). The security of specific DAG-based networks is contingent upon the level of engagement of their network participants (Pervez et al., 2018). DAG-based methods encounter limitations stemming from their relatively recent introduction, as they emerged after traditional blockchains, resulting in less time to establish security across diverse challenging scenarios (Pervez et al., 2018).

4. Hybrid Consensus Approaches for Blockchain in IoT Applications

Hybrid consensus systems signify a significant advancement in blockchain engineering, addressing the challenges faced by traditional consensus protocols in the deployment of IoT applications (Bommireddy, 2024). Hybrid consensus mechanisms integrate two distinct consensus systems to enhance performance characteristics, combining security measures with energy efficiency, scalability, and transaction rate

capabilities (Zhuang et al., 2024). Figure 3 below provides a graphical representation of the fundamental trade-off inherent in hybrid consensus, demonstrating that hybrid methods achieve a superior balance between network security and scalability.

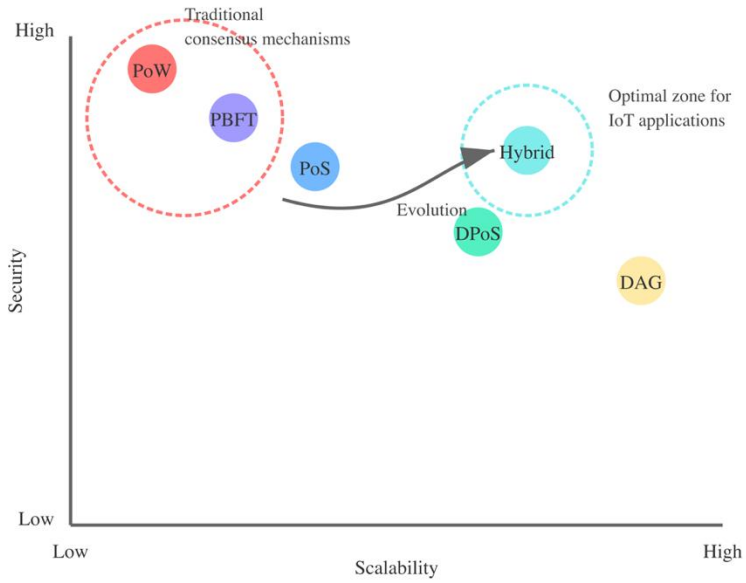

Figure 3. Overview of Security and Scalability trade-off mechanisms

Hybrid mechanisms of Proof-of-Work (PoW) and Proof-of-Stake (PoS) illustrate the integration of distinct proof-of-identity systems to enhance efficiency and minimize power consumption (Zhuang et al., 2024). The primary implementation method employs Proof of Work for block validation, while Proof of Stake is utilized for governance tasks and consensus processes (Aggarwal & Kumar, 2021). The integration of Proof of Work (PoW) and Proof of Stake (PoS) offers a strategy to reduce the significant energy consumption associated with traditional PoW protocols. The PoS component decreases the overall computational demands, thereby enhancing feasibility for specific Internet of Things (IoT) hardware. Hybrid mechanisms must mitigate combined weaknesses while circumventing centralization risks inherent in specific Proof of Stake implementations and demonstrating greater energy efficiency compared to conventional PoS systems, as noted by Alkhateeb et al. (2022).

Routh and Thungon (2024) elaborate that practical Byzantine fault tolerance (PBFT) is integrated with either proof of stake (PoS) or proof of work (PoW) elements in hybrid solutions to enhance system compatibility with IoT applications. The integration of Proof of Stake (PoS) for leader selection in PBFT consensus rounds enhances the fairness of the PBFT process and reduces security vulnerabilities associated with a static main leader. The integration of PBFT with PoW security systems enhances robustness, as the computational complexity of PoW addresses challenging tasks, while PBFT facilitates rapid execution of other operations. Hierarchical consensus methods provide distinct solutions to the challenges of blockchain implementation in extensive IoT networks. These models categorize system components into distinct layers, clusters, or tiers, utilizing various consensus mechanisms based on the attributes of each network level. Resource-constrained IoT devices utilize efficient and lightweight consensus mechanisms to minimize local overhead, whereas higher network tiers implement robust security protocols to ensure comprehensive protection of the IoT network. This hierarchical method significantly decreases the workload on IoT devices by facilitating the sharing of computational and communication tasks. Incorporating reputation-based systems at each network layer offers authentication capabilities that protect devices within clusters, thereby improving the overall resilience

of IoT systems. Figure 4 demonstrates the approach of hierarchical consensus models in tackling blockchain scalability issues within large IoT networks. This is achieved through a layered system architecture, where cluster divisions function independently, employing distinct consensus mechanisms tailored to their specific needs.

.

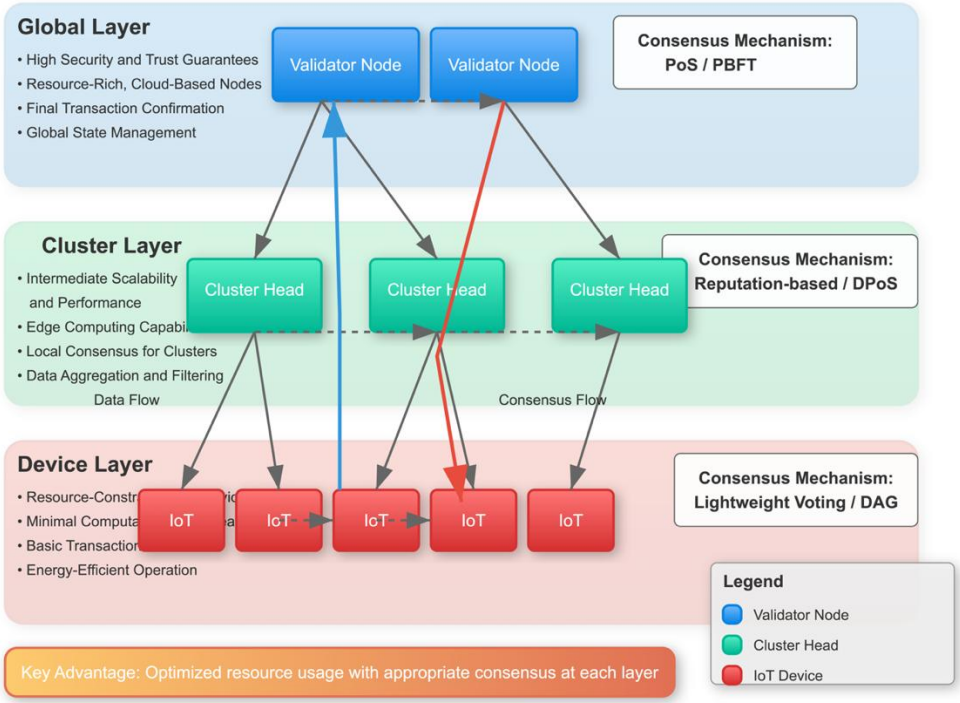

Figure 4. Hierarchical Hybrid Consensus Architecture for IoT environments

Figure 4 illustrates the Hierarchical Hybrid Consensus Architecture, outlining the structure for implementing blockchain consensus in IoT environments across multiple tiers. This design categorizes distinct consensus methods into three operational levels based on device capabilities and network requirements. Validator nodes equipped with sensors operate at the highest tier of the Global Layer, functioning within cloud and edge server infrastructures. Consensus mechanisms such as Proof-of-Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT) function within these nodes to update the global blockchain state and finalize transaction validations. The cluster layer serves as an intermediary between IoT devices and global validators via its cluster head nodes, which possess moderate computational processing capabilities. This layer utilizes DPoS or reputation-based consensus mechanisms to aggregate transactions, prevalidate them, and execute cluster management tasks. The foundational layer consists of the characteristics of typical resource-constrained IoT devices, which gather initial data and perform basic transactions. Consensus approaches are primarily lightweight solutions that utilize either voting strategies or directed acyclic graph (DAG) structures to reduce the computational demands and energy costs associated with these devices. The data within the system originates from IoT devices, progresses to cluster heads, and culminates in global validators, whose decisions are disseminated throughout each layer. A well-structured system design facilitates efficient resource management among IoT devices with varying capabilities and security frameworks, enabling scalable operations within the constraints of limited IoT resources.

Hybrid reputation systems are a widely adopted approach that incorporate the reputation scores of nodes into consensus functions, effectively embedding trust features within the process. (Zhuang et al., 2024).

During the consensus process, ratings that reflect the trustworthy and dependable performance of nodes are utilized to identify those with strong reputations, which in turn influences the extent of power a node holds in consensus operations or critical block validation procedures. The reputation scoring system functions as a protective mechanism by allowing the network to reduce the involvement of nodes that have demonstrated unreliability. The reputation score of a node increases through effective collaboration within the network and adherence to established standards. The integration of a reputation-based secure approach with Proof-of-Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT) results in more flexible secure consensus protocols, which are increasingly appropriate for IoT deployments involving numerous untrusted users.

Urgent Hybrid IoT applications, including Augmented Reality, Virtual Reality, and Industrial IoT, require time-sensitive hybrid mechanisms to facilitate very low latency near-real-time transaction processing. This technology is optimally designed for industrial automation and autonomous systems. (Zhuang et al., 2024). Hybrid consensus approaches consist of various consensus systems that provide rapid finality, such as PBFT and voting protocols, combined with mechanisms that improve data protection. The transaction process utilizes rapid consensus methods for sensor data and control commands, while slower but more secure blockchain anchoring methods are employed periodically. This approach can fulfill the dual requirements of speed and security in specific IoT applications. To implement security mechanisms on time-sensitive IoT devices, it is essential that they function with high efficiency in terms of resource utilization.

5. Case Studies and Implementations in IoT

Numerous studies have investigated hybrid consensual mechanisms to address specific challenges associated with the application of blockchain technology in IoT environments (Barrera et al., 2023). This case study offers insights into the practical benefits and capabilities associated with the implementation of these methods. IOTA exemplifies a distinctive implementation that diverges from conventional blockchain structures by employing a directed acyclic graph (DAG) for its ledger generation (Alhavan et al., 2022). In the network, each new transaction is essential for verifying prior transactions and establishing a web of interconnected transactions. A key feature of IOTA is its objective to facilitate transactions for microtransactions, which are expected to be prevalent in numerous IoT applications (UDDIN et al., 2021). The intake structure is engineered to ensure high scalability and transaction throughput through its parallel processing capabilities (Raikwar et al., 2024). The introduction of additional transactions to the community correlates with an increase in the rate of transaction validation (Ahuja et al., 2015). IOTA employs a light evidence mechanism (POW) primarily to deter unsolicited postal and dishonest transactions, rather than functioning as a fundamental consensual mechanism (UDDIN et al., 2021). The IOTA platform has been investigated for various IoT applications, including decentralized identification control, stable data management in smart agriculture, supply chain monitoring, and the development of intelligent city infrastructure (Pullo et al., 2023).

IoTeX's Roll-DPoS consensus mechanism is specifically designed to enhance scalability and efficiency in Internet of Things (IoT) environments (Coinbase). This system employs a randomly selected delegated Proof-of-Stake mechanism, wherein a predetermined number of representatives are randomly selected to generate new blocks (Fan & Chai, 2018). The selection process for establishing a pool of validator nodes utilizes a community voting mechanism (Chai et al.). IoTeX features an EVM-compatible blockchain, enabling the use of smart contracts (The Cryptonomist, 2024). The objective is to empower self-sovereign IoT devices and applications, focusing on user privacy and data management (Coinbase). Roll-DPoS addresses the challenges of scalability and decentralization encountered when adapting traditional DPoS to a large, heterogeneous resource environment such as IoT (Chai et al.) by implementing a more dynamic and less predictable block producer selection process. Hyperledger Fabric is a permissioned blockchain

framework specifically developed for enterprise-level IoT applications that require stringent privacy and access control measures (Alkurdi et al., 2018). Advanced controls for privacy and organizational policies for fine-grained access are essential requirements for numerous industrial IoT applications (Jarwar et al., 2023). The system features pluggable consensus mechanisms, enabling organizations to tailor their blockchain operations accordingly (IBM, 2021b). The extension is implemented to safeguard data collection, storage, and sharing across various IoT environments, leading to improvements in security, efficiency, and overall system capacity (Honar Pajooh et al., 2021). Research indicates its potential to achieve high transaction throughput, particularly through specific optimizations (Honar Pajooh et al., 2022).

Additionally, a significant application of the hybrid consensus method for blockchain in the Internet of Things is the reputation-based hybrid consensus mechanism (HCM) utilized in electronic healthcare systems (EHS) (Prabha & Chatterjee, 2022). This HCM employs a combination of algorithms for block creation, validation, fork handling, Merkle tree construction, and a reward/punishment module, all based on the activities observed among the various blocks within the system. The H-chain framework is another example, specifically designed for IoT ecosystems comprising various collaborating organizations (Hu et al., 2021). Routh and Thungon (2024) proposed a hybrid blockchain that integrates private blockchain instances employing Practical Byzantine Fault Tolerance (PBFT) with a public blockchain utilizing a permissioned Proof of Work (PoW) consensus mechanism. This design aims to balance the requirements for private transaction verification and the necessity for public, auditable information. This consensus algorithm, proposed for IoT applications utilizing blockchain, aims to enhance scalability via master node election and a restricted broadcast domain, rendering it appropriate for resource-constrained IoT devices (Uddin et al., 2021). Microchain presents a high-level architecture for a lightweight hierarchical consensus protocol tailored for IoT, which incorporates Proof of Concept (PoC) alongside a Voting-based Chain Finality (VCF) consensus protocol (Xu et al., 2020) for block generation. This paper presents a hierarchical, location-aware consensus protocol, termed LH-Raft, designed for IoT-blockchain applications. It establishes local consensus groups based on the reputation and local information of nodes, thereby enhancing network scalability and reducing communication costs (Guo et al., 2022; Guo et al., 2021). This variation in implementations underscores the continuous research and innovation surrounding hybrid consensus mechanisms, which are adapted to meet the diverse requirements and constraints of various IoT application domains, ranging from sensitive healthcare data management to large-scale industrial control systems (Kumari et al. 2025).

6. Performance Analysis and Comparison

A comprehensive framework is required for the performance evaluation of hybrid consensus mechanisms in IoT applications, utilizing various performance metrics. Key characteristics include energy efficiency, crucial for resource-constrained IoT devices; scalability, which refers to the capacity to handle numerous devices and significant transaction volumes; transaction throughput, measured as transactions processed per second; security guarantees, indicating the resilience of the mechanism against various attacks typical in IoT environments; fault tolerance, the capacity to maintain functionality despite node failures or malicious actions; and latency features, the time required for a transaction to be verified and integrated into the blockchain (Al Ahmed et al., 2022). Each approach presents trade-offs, as detailed in an analysis of various hybrid consensus mechanisms based on these key metrics. Various design iterations, such as PoW/PoS hybrids, exhibit medium energy efficiency, medium scalability, and transaction throughput, alongside high to medium security guarantees and fault tolerance. These systems can be categorized as either probabilistic (PoW-based) or stake-based (PoS-based), with medium-high latency characteristics. PBFT integrated with PoS or PoW components exhibits moderate energy efficiency and scalability, while achieving medium to high throughput, alongside robust security and fault tolerance, and low to medium latency (Singh & Nandi, 2023). Hierarchical consensus models generally provide medium to high energy

efficiency and scalability, alongside medium to high throughput, security, and fault tolerance, which fluctuate based on the layer, and exhibit medium to low latency. Reputation-based hybrids typically exhibit medium to high energy efficiency and scalability, alongside medium to high throughput. They also offer improved security and fault tolerance attributed to the reputation system, while latency remains medium to low. Time-sensitive hybrids emphasize low latency while achieving high throughput, exhibiting medium energy efficiency and scalability. Security and fault tolerance vary based on the specific combination of mechanisms employed. Hierarchical consensus models generally provide medium to high energy efficiency and demonstrate excellent scalability, accompanied by medium to high throughput. Their security and fault tolerance are contingent upon the specific layer implementation, exhibiting medium to low latency. Reputation-based hybrids typically demonstrate favorable energy efficiency and scalability, achieving medium to high throughput alongside improved security and fault tolerance attributed to their reputation systems, while maintaining medium to low latency. Time-sensitive hybrids emphasize low latency and high throughput, achieving medium energy efficiency and scalability, while security and fault tolerance are contingent upon the specific mechanisms employed.

DAG-based approaches, such as IOTA's Tangle, are engineered for enhanced energy efficiency, scalability, and throughput. Their security relies on network activity and the fault tolerance characteristic of the DAG structure, resulting in low latency. IoTeX's Roll-DPoS seeks to enhance energy efficiency, scalability, and throughput through stake-based security and delegate-based fault tolerance, resulting in low latency (Coinbase). Hyperledger Fabric features configurable consensus mechanisms that influence its performance characteristics. It typically provides medium scalability, high throughput, and security designed for permissioned networks, alongside adjustable fault tolerance and low latency. The reputation-based HCM exhibits moderate energy efficiency, scalability, and throughput, while also providing enhanced security and improved fault tolerance through its reputation module, alongside medium latency. The H-chain integrates Proof of Work (PoW) and Practical Byzantine Fault Tolerance (PBFT), demonstrating variable energy efficiency and moderate scalability, alongside medium throughput, high security and fault tolerance, and medium latency. CBCIoT, a voting-based mechanism, demonstrates high energy efficiency, scalability, and throughput, alongside rating-based security, majority-based fault tolerance, and low latency. Table 1 presents a summary of the performance comparison among various hybrid consensus mechanisms for IoT.

Table 1: Performance Comparison of Hybrid Consensus Mechanisms for IoT

Mechanism	**Energy Efficiency**	**Scalability**	**Throughput**	**Security Guarantees**	**Fault Tolerance**	**Latency**
PoW/PoS Hybrids	Medium	Medium	Low to Medium	High to Medium	Probabilistic to Stake-based	Medium to High
PBFT with PoS/PoW	Medium	Low to Medium	Medium to High	High	High	Low to Medium
Hierarchical Consensus Models	Medium to High	High	Medium to High	Varies by layer	Varies by layer	Medium to Low

Reputation-based Hybrids	Medium to High	Medium to High	Medium to High	Enhanced by reputation	Improved	Medium to Low
Time-sensitive Hybrids	Medium	Medium	High	Varies by combination	Varies by combination	Low
IOTA's Tangle	High	High	High	Depends on network activity	Inherent in DAG structure	Low
IoTeX's Roll-DPoS	High	High	High	Stake-based	Delegate-based	Low
Hyperledger Fabric (Configurable)	Varies	Medium	High	Permissioned, Configurable	Configurable	Low
HCM (Reputation-based)	Medium	Medium	Medium	Enhanced by reputation	Improved	Medium
H-chain (PoW/PBFT)	Varies	Medium	Medium	High	High	Medium
CBCIoT (Voting-based)	High	High	High	Rating-based	Majority-based	Low

The combination of algorithms, network architecture, and characteristics of IoT devices significantly impacts the effectiveness of hybrid consensus mechanisms in IoT. The absence of a universal solution necessitates that the selection of the most suitable mechanism is contingent upon a thorough evaluation of the specific needs and constraints of the application's context. It is crucial to consider limiting factors such as energy constraints, scalability requirements, security needs, and latency tolerance in order to derive the most suitable hybrid consensus for a specific Internet of Things application.

7. Open Challenges and Future Directions

Significant challenges remain as recent advancements in hybrid consensus protocols for blockchain technology, particularly in IoT applications, present several unresolved issues that require attention. A significant obstacle is the need to standardize consensus among hybrids to enable widespread deployment and interoperability at the IoT level (George, 2024). This may complicate integration if different versions lack shared standards or protocols, potentially limiting the reuse of solutions offered by other software vendors. Standardization of interfaces, data formats, and security requirements in Internet of Things (IoT) consensus hybrids is essential. This indicates the development of a more cohesive and interoperable ecological system. The absence of universally accepted standards leads to fragmentation, resulting in individual solution investments being hindered by vendor lock-in. The potential for

breakthroughs is constrained due to a lack of interoperability. A significant consideration is the presence of security vulnerabilities (Zhuang et al., 2024). Proof-of-Work and Proof-of-Stake represent the two primary consensus protocols, while hybrid mechanisms frequently integrate various protocols to enhance security. The complexity of these hybrids and their combinations may inadvertently lead to additional weaknesses and attack vectors. A thorough security assessment and rigorous testing of a blockchain-based IoT system design are essential for identifying and addressing vulnerabilities to ensure overall robustness. A thorough analysis of the interactions among diverse consensus components is essential to guarantee that the overall system does not exhibit diminished strength compared to the individual components. Significant scalability barriers persist, particularly in large-scale IoT deployments that encompass billions of devices and exceptionally high transaction rates (Ragul et al., 2025). While few mixed systems demonstrate superior scalability compared to traditional mechanisms, considerable research and development are required to adapt these systems to effectively address the demands of large IoT networks, particularly concerning limited and low-latency information processing. The scalability of blockchain-based IoT solutions utilizing hybrid consensus mechanisms remains a developing area.

Nonetheless, it presents specific opportunities and risks. Transitioning to architectures with distributed processing capabilities may enhance the efficiency and scalability of hybrid consensus, which has been a challenge to attain. This transition involves addressing issues related to data consistency, security, and synchronization across different layers in diverse distributed environments (Abdulrahman et al., 2025). Ensuring seamless and secure interfacing between the blockchain layer and distributed computing architectures is a complex issue. The regulatory implications of integrating blockchain with IoT are becoming more substantial. This encompasses hybrid consensus mechanisms (Zorrilla & Yebenes, 2022). Consideration of existing and potential regulatory frameworks for data privacy, security, and governance is essential. Adhering to regulations such as GDPR, which grant users the right to modify or delete their data, poses significant challenges due to the immutable characteristics of blockchain ledgers (Liu et al., 2022). Hybrid mechanisms may require the integration of enforcement measures that fulfill such requirements while preserving the fundamental advantages of blockchain technology (Atlam et al., 2018).

8. Conclusion

The integration of blockchain technology with the Internet of Things presents significant potential for enhancing the security of interconnected systems that are increasingly vulnerable to hacking and data tampering. Despite the numerous traditional consensus mechanisms proposed for blockchain, none have effectively addressed the specific requirements of IoT. The emergence of hybrid consensus approaches may alter this situation. These mechanisms strategically integrate the benefits of various consensus protocols to balance energy efficiency with scalability, throughput with security and fault tolerance, as well as latency, thereby aligning with the specific requirements of diverse IoT applications. The landscape of hybrid consensus mechanisms includes various models such as PoW/PoS hybrids, PBFT integrated with PoS or PoW elements, hierarchical consensus models, reputation-based approaches, and time-sensitive hybrid mechanisms. Applications including IOTA's Tangle, IoTeX's Roll-DPoS, and Hyperledger Fabric for IoT exemplify innovation across various domains. A comparative performance analysis highlighted the trade-offs inherent in each approach, emphasizing that results varied significantly based on the specific requirements of the IoT application. Despite the advancements achieved, several unresolved questions remain to be addressed. Compatibility standards continue to hinder intercommunication, and vulnerabilities in complex hybrid designs require comprehensive investigation. Challenges concerning scalability for large-scale IoT implementations, integration with new IoT frameworks, and adaptation to a dynamic legal landscape remain unresolved. Future research should concentrate on developing standardized frameworks for hybrid consensus in IoT, accompanied by thorough security analyses of existing and novel methodologies. Additionally, efforts should aim at achieving scalability for ultra-scale IoT networks, ensuring seamless integration with edge and fog computing paradigms, and formulating

blockchain solutions that comply with IoT regulations. Practitioners must conduct a comprehensive examination of the specific requirements pertinent to their IoT applications. Factors such as the device's resource limitations, the level and type of data to be processed and stored, and potential security requirements must be considered when selecting an appropriate hybrid consensus mechanism. Examining the integration of blockchain technology with security necessitates a detailed analysis of the associated performance trade-offs. The open problems, whether arising from diverse perspectives or insufficient resources to address them, require thorough examination commensurate with their understanding.

Acknowledgements
The authors declare that, there is no financial support from any of the institutions or personal relationship to affect the quality of the paper.

Conflicts of Interest
The authors declare no conflicts of interest.

Author Contributions
Dr. N. A. Natraj: Conceptualization, methodology, validation, writing – original draft. **Dr. Midhunchakkaravarthy, J. J.**: Data curation, formal analysis, investigation, writing – review and editing, supervision. **Dr. Brojo Kishore Mishra**: Resources, visualization, writing – review, project administration. **Ms. Supriya Laykar:** writing – review and editing

Data Availability Statement
The data supporting the findings of this study is openly available. The survey analysis was performed using publicly accessible research articles, technical documentation, and case studies, all of which are cited throughout the manuscript. No new datasets were generated during this research. Performance comparison data was compiled from the referenced literature and standardized for comparative analysis. Implementation details and metrics for the case studies were obtained from official documentation, published research papers, and open-source repositories. All sources are properly cited and available through their respective publishers or repositories. Additional information regarding the performance metrics framework is available upon reasonable request from the corresponding author.

Funding Information
No Funding was received for this research.

References
1. Pal, S., Hitchens, M., Rabehaja, T. M., & Mukhopadhyay, S. C. (2020). Security Requirements for the Internet of Things: A Systematic Approach. *Sensors*, *20*(20), 5897. https://doi.org/10.3390/S20205897
2. Alhavan, M., Azimi, A., & Corchado, J. M. (2022). A CoviReader Architecture Based on IOTA Tangle for Outbreak Control in Smart Cities during COVID-19 Pandemic. *Medical Journal of the Islamic Republic of Iran*, *36*. https://doi.org/10.47176/mjiri.36.180
3. Dirin, A., Oliver, I., & Laine, T. H. (2023). A Security Framework for Increasing Data and Device Integrity in Internet of Things Systems. *Sensors*, *23*(17), 7532. https://doi.org/10.3390/s23177532
4. Anosike, C. N., Adeleke, O. J., Adediji, A. P., Okereke, R. O., Cynthia, U. C., & Sodipe, A. O. Research Title: Review Of Iot Device Security, Methods To Enhance Security And Prevent Cyber Attacks And Data Breaches. *Authorea.* August 28, 2024. 10.22541/au.172481288.88002325/v1
5. Zorrilla, M., & Yebenes, J. (2022). A reference framework for the implementation of data governance systems for industry 4.0. Computer Standards & Interfaces, 81, 103595. https://doi.org/10.1016/j.csi.2021.103595

6. Sulaeman, A. A. (2025). Blockchain-Powered Security Framework for IoT Data Integrity and Privacy. The Journal of Academic Science, 2(3), 874-882. https://thejoas.com/index.php/thejoas/article/view/285
7. Oh, T. (2025). Blockchain-Enabled Security Enhancement for IoT Networks: Integrating LEACH Algorithm and Distributed Ledger Technology. *Journal of Machine and Computing*, 483–495. https://doi.org/10.53759/7669/jmc202505038
8. Verma, R., Thakur, S., Vaidya, P., & Sharma, B. B. (2024, November). Blockchain-Enabled IoT: Revolutionizing Security and Data Integrity in Connected Devices. In 2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON) (pp. 1-5). IEEE.
9. Almarri, S., & Aljughaiman, A. (2024). Blockchain Technology for IoT Security and Trust: A Comprehensive SLR. *Sustainability*, *16*(23), 10177. https://doi.org/10.3390/su162310177
10. Alkurdi, F., Elgendi, I., Munasinghe, K. S., Sharma, D., & Jamalipour, A. (2018, November). Blockchain in IoT security: a survey. In 2018 28th International Telecommunication Networks and Applications Conference (ITNAC) (pp. 1-4). IEEE.
11. Ahakonye, L. A. C., Nwakanma, C. I., & Kim, D. S. (2024). Tides of Blockchain in IoT Cybersecurity. Sensors (Basel, Switzerland), 24(10), 3111. https://doi.org/10.3390/s24103111
12. Vavilis, S., Niavis, H., & Loupos, K. (2025). A Fair and Lightweight Consensus Algorithm for IoT. arXiv preprint arXiv:2503.08607.
13. Ragul, M., Aloysius, A., & Kumar, V. A. (2025). Enhancing IoT blockchain scalability through the eepos consensus algorithm. The Scientific Temper, 16(1), 3698–3709. https://doi.org/10.58414/SCIENTIFICTEMPER.2025.16.1.16
14. Zhuang, Y., Chen, Y., Zhang, X., Ren, T., Han, M., Alam, M., & Hong, Z. (2024). A Large-Scale Node Lightweight Consensus Algorithm of Blockchain for Internet of Things. *IEEE Internet of Things Journal*.
15. Bommireddy, N. R. (2024). Consensus for Creating Light Weight Blockchain for IoT. Southern Illinois University at Carbondale.
16. Haque, E. U., Abbasi, W., Almogren, A., Choi, J., Altameem, A., Rehman, A. U., & Hamam, H. (2024). Performance enhancement in blockchain based IoT data sharing using lightweight consensus algorithm. Scientific reports, 14(1), 26561. https://doi.org/10.1038/s41598-024-77706-x
17. Hsueh, C.-W., & Chin, C.-T. (2023). Toward Trusted IoT by General Proof-of-Work. Sensors, 23(1), 15. https://doi.org/10.3390/s23010015
18. Lepore, C., Ceria, M., Visconti, A., Rao, U. P., Shah, K. A., & Zanolini, L. (2020). A survey on blockchain consensus with a performance comparison of PoW, PoS and pure PoS. Mathematics, 8(10), 1782.
19. Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE access, 7, 85727-85745.
20. Khan, M., den Hartog, F., & Hu, J. (2022). A Survey and Ontology of Blockchain Consensus Algorithms for Resource-Constrained IoT Systems. Sensors (Basel, Switzerland), 22(21), 8188. https://doi.org/10.3390/s22218188
21. Sapra, N., Shaikh, I., & Dash, A. (2023). Impact of proof of work (PoW)-Based blockchain applications on the environment: a systematic review and research agenda. *Journal of Risk and Financial Management*, *16*(4), 218.
22. Amin, M. R. (2020). 51% attacks on blockchain: a solution architecture for blockchain to secure iot with proof of work. *Bachelor Thesis, International University of Business Agriculture and Technology, Dhaka, Bangladesh*.
23. Parmar, M., & Kaur, H. J. (2021). Blockchain-Enabled Consensus Routing Protocol Improving the Security Data Communication in Internet of Things Applications. *International Journal of Computer Networks and Applications*, *8*(4), 268-276.
24. Liu, S., Zhang, R., Liu, C., Xu, C., & Wang, J. (2023). An improved PBFT consensus algorithm based

on grouping and credit grading. *Scientific reports*, *13*(1), 13030. https://doi.org/10.1038/s41598-023-28856-x
25. Qi, J., & Guan, Y. (2023). Practical Byzantine fault tolerance consensus based on comprehensive reputation. Peer-to-Peer Networking and Applications, 16(1), 420-430.
26. Yuan, F., Huang, X., Zheng, L., Wang, L., Wang, Y., Yan, X., Gu, S., & Peng, Y. (2025). The Evolution and Optimization Strategies of a PBFT Consensus Algorithm for Consortium Blockchains. *Information*, *16*(4), 268. https://doi.org/10.3390/info16040268
27. Ankan Routh, Leki Chom Thungon. IoTSecChain: Advancing IoT Network Communications with PBFT Consensus and ECC Authentication. Authorea. November 20, 2024. 10.22541/au.173210446.67966051/v1
28. Singh, R., & Nandi, S. (2023, May). An improved pbft-based consensus protocol for industrial iot. In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)* (pp. 311-312). IEEE.
29. Uddin, M., Muzammal, M., Hameed, M. K., Javed, I. T., Alamri, B., & Crespi, N. (2021). CBCIoT: a consensus algorithm for blockchain-based IoT applications. *Applied Sciences*, *11*(22), 11011.
30. Raikwar, M., Polyanskii, N., & Müller, S. (2024, May). SoK: DAG-based Consensus Protocols. In *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1-18). IEEE.
31. Pervez, H., Muneeb, M., Irfan, M. U., & Haq, I. U. (2018, December). A comparative analysis of DAG-based blockchain architectures. In *2018 12th International conference on open source systems and technologies (ICOSST)* (pp. 27-34). IEEE.
32. de Morais, A. M., Lins, F. A. A., & Rosa, N. S. (2023). Survey on integration of consensus mechanisms in IoT-based blockchains. *Journal of Universal Computer Science*, *29*(10), 1139.
33. Prabha, P., & Chatterjee, K. (2022). Design and implementation of hybrid consensus mechanism for IoT based healthcare system security. *International Journal of Information Technology*, *14*(3), 1381-1396.
34. Hu, J., Reed, M. J., Al-Naday, M., & Thomos, N. (2021). Hybrid blockchain for IoT—Energy analysis and reward plan. *Sensors*, *21*(1), 305.
35. Aggarwal, S., & Kumar, N. (2021). Cryptographic consensus mechanisms. In *Advances in computers* (Vol. 121, pp. 211-226). Elsevier.
36. Kumari, T., Kumar, R., & Dwivedi, R. K. (2025). Blockchain-based secure and smart healthcare iot system using hybrid consensus mechanism with an honest block. *Health Services and Outcomes Research Methodology*, *25*(1), 113-151.
37. Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review. *Sensors*, *22*(4), 1304.
38. Wingreen, S. C., Kavanagh, D., Dylan-Ennis, P., & Miscione, G. (2020). Sources of cryptocurrency value systems: the case of Bitcoin. *International Journal of Electronic Commerce*, *24*(4), 474-496.
39. Tanwar, S. (2018). Blockchain technology. *Blockchain Regulation and Governance in Europe*.
40. Jaradat, A., Ali, O., & AlAhmad, A. (2021). Blockchain technology: a fundamental overview. In *Blockchain technologies for sustainability* (pp. 1-24). Singapore: Springer Singapore.
41. What Is Blockchain? | IBM. (2021). https://www.ibm.com/think/topics/blockchain
42. *What Is Blockchain and How Does It Work? | Black Duck*. (n.d.). https://www.blackduck.com/glossary/what-is-blockchain.html
43. Eze, K. G., Akujuobi, C. M., Sadiku, M. N., Chouikha, M., & Alam, S. (2019). Internet of things and blockchain integration: Use cases and implementation challenges. In *Business Information Systems Workshops: BIS 2019 International Workshops, Seville, Spain, June 26–28, 2019, Revised Papers 22* (pp. 287-298). Springer International Publishing.
44. Gupta, S., Hellings, J., Rahnama, S., & Sadoghi, M. (2019, December). An in-depth look of BFT consensus in blockchain: Challenges and opportunities. In *Proceedings of the 20th international middleware conference tutorials* (pp. 6-10).

45. Kim, H., & Kim, D. (2023). A taxonomic hierarchy of blockchain consensus algorithms: An evolutionary phylogeny approach. *Sensors*, *23*(5), 2739.
46. Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications*, *125*, 251-279.
47. George, I. (2024). Exploring the Integration of Blockchain in IoT Use Cases: Challenges and Opportunities
48. Atlam, Hany F., Ahmed Alenezi, Madini O. Alassafi, and Gary Wills. "Blockchain with internet of things: Benefits, challenges, and future directions." *International Journal of Intelligent Systems and Applications* 10, no. 6 (2018): 40-48.
49. Obaidat, M. A., Rawashdeh, M., Alja'afreh, M., Abouali, M., Thakur, K., & Karime, A. (2024). Exploring IoT and Blockchain: A Comprehensive Survey on Security, Integration Strategies, Applications and Future Research Directions. *Big Data and Cognitive Computing*, *8*(12), 174.
50. Qu, X., Wang, S., Li, K., Huang, J., & Cheng, X. (2024). TidyBlock: A Novel Consensus Mechanism for DAG-based Blockchain in IoT. *IEEE Transactions on Mobile Computing*.
51. Khan, M., Hartog, F. D., & Hu, J. (2024). Toward verification of DAG-based distributed ledger technologies through discrete-event simulation. *Sensors*, *24*(5), 1583.
52. Sealey, N., Aijaz, A., & Holden, B. (2022, November). IOTA tangle 2.0: Toward a scalable, decentralized, smart, and autonomous IoT ecosystem. In *2022 International Conference on Smart Applications, Communications and Networking (SmartNets)* (pp. 01-08). IEEE.
53. Ahuja, S., Johari, R., & Khokhar, C. (2015, September). IoTA: Internet of things application. In *Proceedings of the Second International Conference on Computer and Communication Technologies: IC3T 2015, Volume 3* (pp. 235-247). New Delhi: Springer India.
54. Pullo, S., Pareschi, R., Piantadosi, V., Salzano, F., & Carlini, R. (2023, December). Integrating iota's tangle with the internet of things for sustainable agriculture: A proof-of-concept study on rice cultivation. In *Informatics* (Vol. 11, No. 1, p. 3). MDPI.
55. Xu, R., Chen, Y., & Blasch, E. (2020). Microchain: A light hierarchical consensus protocol for iot systems. In *Blockchain Applications in IoT Ecosystem* (pp. 129-149). Cham: Springer International Publishing.
56. Al Ahmed, M. T., Hashim, F., Hashim, S. J., & Abdullah, A. (2022). Hierarchical blockchain structure for node authentication in IoT networks. *Egyptian Informatics Journal*, *23*(2), 345-361.
57. Guo, H., Li, W., & Nejad, M. (2022). A hierarchical and location-aware consensus protocol for IoT-blockchain applications. *IEEE Transactions on Network and Service Management*, *19*(3), 2972-2986.
58. Guo, H., Li, W., & Nejad, M. (2021, November). A location-based and hierarchical framework for fast consensus in blockchain networks. In *2021 4th International Conference on Hot Information-Centric Networking (HotICN)* (pp. 1-6). IEEE.
59. Ramírez-Gordillo, T., Maciá-Lillo, A., Pujol, F. A., García-D'Urso, N., Azorín-López, J., & Mora, H. (2025). Decentralized Identity Management for Internet of Things (IoT) Devices Using IOTA Blockchain Technology. *Future Internet*, *17*(1), 49.
60. IoTeX Price, IOTX Price, Live Charts, and Marketcap – Coinbase, https://www.coinbase.com/price/iotex
61. Chai, R., Guo, Q., Sun, J., & Fan, X. (n.d.). An Overview of IOTEX (Iotx). Retrieved March 28, 2025, from https://pontem.network/posts/an-overview-of-iotex-iotx
62. *The report by Messari on the IoTex platform update: the DePIN sector advances*. (2024, November 18). The Cryptonomist. https://en.cryptonomist.ch/2024/11/18/the-report-by-messari-on-the-iotex-platform-update-the-depin-sector-advances/
63. Fan, X., & Chai, Q. (2018, November). Roll-DPoS: a randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems. In *Proceedings of the 15th EAI international conference on mobile and ubiquitous systems: computing, networking and services* (pp. 482-484).

64. Honar Pajooh, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Hyperledger fabric blockchain for securing the edge internet of things. *Sensors*, *21*(2), 359.
65. What Is Hyperledger Fabric? | IBM. (2021, July 16)., https://www.ibm.com/think/topics/hyperledger
66. Jarwar, M. A., Ali, S., & Shah, S. C. (2023, December). Taking IoT Security to the Next Level: Hyperledger Fabric Private Blockchain Enabled IoT Middleware. In *2023 IEEE Globecom Workshops (GC Wkshps)* (pp. 1325-1330). IEEE.
67. Honar Pajooh, H., Rashid, M. A., Alam, F., & Demidenko, S. (2022). Experimental Performance Analysis Of A Scalable Distributed Hyperledger Fabric For A Large-Scale IoT testbed. *Sensors*, *22*(13), 4868.
68. Abdulrahman, E., Alshehri, S., Alzubaidy, A., & Cherif, A. (2025). A Distributed Blockchain-based Access Control for the Internet of Things. *arXiv preprint arXiv:2503.17873*.
69. Barrera, D., Bellman, C., & Van Oorschot, P. (2023). Security best practices: a critical analysis using IoT as a case study. *ACM Transactions on Privacy and Security*, *26*(2), 1-30.