EAI Endorsed Transactions
on Internet of Things

Research Article EAI.EU

A Quantitative Framework for the Selection of Hybrid Consensus Mechanisms in Blockchain-IoT Systems

N. A. Natraj[1]*, Midhunchakkaravarthy, J. J.[3], and Brojo Kishore Mishra[3]

[1]Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University), Pune, Maharashtra, India,
[2]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

Abstract

INTRODUCTION: The application of blockchain technology to Internet of Things (IoT) systems offers substantial potential for enhancing security, but traditional consensus mechanisms are ill-suited for resource-constrained environments. While hybrid consensus solutions have emerged as a promising alternative, a systematic framework for their classification and evaluation is notably absent.
OBJECTIVES: This study addresses this critical gap by introducing a novel, application-driven framework for analyzing hybrid consensus mechanisms, underpinned by a quantitative synthesis of performance benchmarks.
METHODS: We analyze diverse architectures—including combinations of Proof of Work (PoW) and Proof of Stake (PoS), PBFT-enhanced systems, and hierarchical models—through the lens of specific IoT application priorities, such as latency, energy efficiency, and scalability. Case studies of IOTA's Tangle, IoTeX's Roll-DPoS, and Hyperledger Fabric illustrate these practical trade-offs.
RESULTS: Our framework reveals not only primary performance trade-offs but also critical "second-order" complexities, such as emergent vulnerabilities at the intersection of different consensus layers.
CONCLUSION: Our findings demonstrate that this structured, quantitatively-grounded approach provides an effective methodology for designing and selecting regulatory-compliant hybrid consensus solutions for specific 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

Received on 11 September 2025, accepted on 10 November 2025, published on 19 November 2025

doi: 10.4108/eetiot.10249

1. Introduction

The Internet of Things has experienced impressive growth because the implementation of connected devices and the resulting addition of bandwidth to the network have spread across the globe [1]. Such a fast development of IoT technologies, in its turn, has spawned a set of new security weaknesses, mostly due to sensitive and critical nature of data such systems produce [1]. To address this, an end-to-end system of operational and security mechanisms has been implemented in the sphere of the IoT to protect data integrity, privacy, hardware quality, and network security [3]. The very nature of IoT operation features, combined with the fact that they process very sensitive data, such as personal financial and healthcare information, requires compliance with such high standards [3]. Lack of strong security functions in the IoT environments initiates unpleasant consequences that go beyond data leakage.

*Corresponding author. Email: natraj@sidtm.edu.in, pdf.natraj@lincoln.edu.my

Open areas of IoT systems may cause severe financial damages and loss of confidence of users in these sites. Therefore, regular systems maintenance is essential to prevent equipment malfunction that is caused by security risks of interconnected systems [3]. The IoT statistics are also essential to facilitate advanced applications based on the industrial IoT and artificial intelligence technologies [5]. Blockchain technology stands out as a new technology that can potentially address essential safety and information integrity issues in IoT systems [8]. The blockchain security system grants decentralization, resulting in tamper resistant and transparent, which improves IoT security and builds trust among the connected devices and users [6]. The immutable records, decentralized functionality of blockchain, and cryptographic security are the primary qualities that enhance the security of IoT networks to protect the data and enable authentic exchange of messages between devices [23]. It can be stated that blockchain technology provides a permanent and traceable history of device interactions, which is guaranteed to be completely authentic and traceable with the data of each element of the IoT network [7]. With the support of smart contracts, which involve the automobile of security measures, blockchain platforms enable authorized access to the IoT data and enhance privacy protection, as reported by Oh [7].

The basic infrastructure established by blockchain will enable companies to build credible decentralized operating frameworks and at the same time protect the IoT landscape [9]. Traditional blockchain consensus algorithms that have been effective elsewhere, however, do not meet the demanding operation criteria of the IoT-based systems, as posed by Kim and Kim [45]. The use of Proof of Work (PoW) and Proof of Stake (PoS) consensus mechanism create a serious problem to the IoT devices as they are computationally intensive and consume a lot of energy which is beyond the capacities of the hardware used by the devices [12]. PoW mining requires a lot of energy usage, particularly when run on battery-powered devices that have limited processing power [12]. This makes PoS systems significantly more energy-efficient than PoW systems, which puts serious challenges on large-scale deployments of IoT networks [41]. The scaling requirement of a large IoT network make Practical Byzantine Fault Tolerance (PBFT) ineffective as the complexity of communication increases with the size of the network [14]. The resource limitations of the IoT devices introduce a strong deviation of the typical blockchain consensus protocols, including POW and POS, which in turn calls upon specific and effective solutions aimed at IoT-specific settings [20].

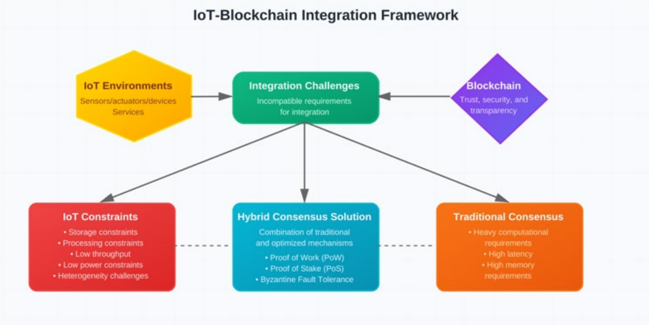


Figure 1. IoT-blockchain integration and the hybrid consensus solution framework

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 [14]. 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 [32]. Combinations of multi-consensus algorithms create hybrid mechanisms that produce robust solutions, addressing specific weaknesses in diverse IoT applications [32]. The study indicates that conventional consensus methods by themselves are insufficient to address the diverse management challenges present in various Internet of Things systems [37].

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.

1.1 Positioning and Contributions Relative to Existing Literature

While several surveys have examined blockchain consensus mechanisms for IoT applications, this work advances the field through distinct contributions that address gaps in existing literature. Table 2 positions our work relative to recent comprehensive surveys in this domain.

Table 1. Comparative Positioning with Recent Survey Literature

Study	Year	Primary Focus	Scope of Coverage	Our Advancement
Khan et al. (2022)	2022	Resource-constrained consensus algorithms	Taxonomy of traditional consensus mechanisms for IoT	Comprehensive analysis of hybrid mechanisms integrating multiple protocols
Zhuang et al. (2024)	2024	Lightweight consensus for large-scale networks	Single lightweight algorithm development	Multi-mechanism integration framework with quantitative trade-off analysis
Almarri & Aljughaiman (2024)	2024	Blockchain for IoT security and trust	General blockchain security applications	Specific hybrid consensus architectures with performance metrics
Proposed Work	2025	Hybrid consensus architectures	7 hybrid mechanism types, 3 implementation case studies, 6 quantitative performance metrics	Systematic framework for hybrid consensus selection, quantitative comparison, and practical deployment guidance

Our work distinguishes itself through four primary contributions. First, we present a comprehensive taxonomy of hybrid consensus mechanisms that have emerged in recent years (2022-2025), including reputation-based systems, time-sensitive frameworks, and hierarchical architectures that have not been systematically analyzed in prior surveys. Second, we establish a structured performance evaluation framework that enables direct quantitative comparison across seven distinct hybrid architectures using six critical metrics specifically relevant to IoT constraints: energy efficiency, scalability, transaction throughput, security guarantees, fault tolerance, and latency. Third, through detailed examination of three contemporary implementations—IOTA's Tangle, IoTeX's Roll-DPoS, and Hyperledger Fabric—we provide practical insights into real-world deployment considerations for healthcare and industrial automation applications. Finally, we identify specific open challenges in standardization, security evaluation, scalability for ultra-large networks, and regulatory compliance, offering actionable directions for future research aligned with emerging IoT-edge computing paradigms.

1.2 Paper Organization

Despite recent surveys on blockchain-IoT integration, this work provides distinct contributions that advance the field. First, we present a systematic taxonomy of hybrid consensus mechanisms that emerged between 2022-2025, including reputation-based, time-sensitive, and hierarchical approaches not comprehensively covered in earlier reviews. Second, we establish a structured performance evaluation framework that enables direct comparison of seven hybrid architectures across six critical metrics specific to IoT constraints. Third, through detailed analysis of three contemporary implementations—IOTA's Tangle 2.0, IoTeX's Roll-DPoS, and Hyperledger Fabric—we provide practical insights into deployment considerations for healthcare and industrial automation applications. Finally, we identify specific open challenges and provide actionable future research directions aligned with emerging IoT-edge computing paradigms and regulatory requirements.

2. Background and Foundational Concepts

Blocks hold transaction information, time stamps and cryptographic hash that makes them connected to the prior blocks [42]. Firstly, networks can be permissioned (limited accessibility among participants) or permissionless (full access); secondly, smart contracts provide automatic implementation of encoded agreements [40].

Visions of consensus mechanisms maintain a consensus state of blockchain networks [9]. They are primarily sought to authenticate transactions and prevent fraud using the protocols of established recording practices that guarantee participant approval, consequently, data coherence and operational integrity [26]. This has resulted in the critical trade-offs between security, speed, scalability, and energy efficiency with the growing diversity of the consensus methods [18]. The traditional ones are the computationally intensive Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerant (PBFT), Proof of Authority (PoA), and Directed Acyclic Graph (DAG)-based ones [19]. Hybrid consensus was identified when the scholars tried to achieve better performance by combining them with traditional strategies [35]. The choice of consensus mechanisms in blockchain networks may be a determinant of their performance and security, and the use of IoT-specific requirements is a crucial factor in this choice [11].

IoT settings comprise thousands to millions of resource-constrained devices with limited processing, storage, and energy capacity [20]. Applications require processing with very high speed and low latency, and the heterogeneity of devices poses a major interoperability problem[13][14]. The most important factor is security because there is need to protect sensitive data against breaches and physical threats against infrastructure [1]. The particularities of IoT also require blockchain solutions to address the limitations that were not of the utmost priority in earlier cryptocurrency settings, as resource shortages and real-time requirements were not as acute [13].

The use of the blockchain technology in the IoT faces a number of challenges. Scalability is an issue since a traditional network is not capable of supporting the enormous amount of devices and data streams [6]. Traditional consensus engines require prohibitive power requirements on battery-powered gadgets [6]. Weaknesses in computing further hinder the implementation of the advanced blockchain protocols [6]. The resultant coherent solution is needed to achieve seamless interoperability between heterogeneous devices in the IoT and blockchain platforms [7]. The integrity of the system needs to be ensured through comprehensive testing and verification of smart contracts, as automated processes have security vulnerabilities that pose risks to the system integrity [43]. The adoption of decentralized state blockchains into IoT systems should find a solution to regulatory uncertainties and adhere to GDPR privacy requirements, which determine the immutability of data [46]. Such technical collaboration thus requires innovation to establish customized consensus mechanisms that make it possible to apply blockchain to the IoT systems practically [49].

3. Limitations of Traditional Consensus Mechanisms in IoT Environments

The use of Proof of Work (PoW) in IoT systems is seen as a challenge [17]. PoW also requires a lot of energy due to solving cryptographic puzzles, which are not compatible with battery- and resource-constrained devices. The computational requirements and specialized hardware needs of PoW exceed the capabilities of IoT peripherals [13]. Additionally, its slow transaction speed and lengthy confirmation durations fail to meet the data validation demands of IoT applications, which are often urgent [17]. The IoT is prone to 51 percent attacks, whereby one party gains a monopoly in the PoW networks through the use of hash power [22]. The principle of PoW is based on extensive computation, which is incompatible with the computational and power constraints of IoT devices, making it unsuitable for massive implementation [13]. Figure 2 illustrates the resources required by various consensus mechanisms.

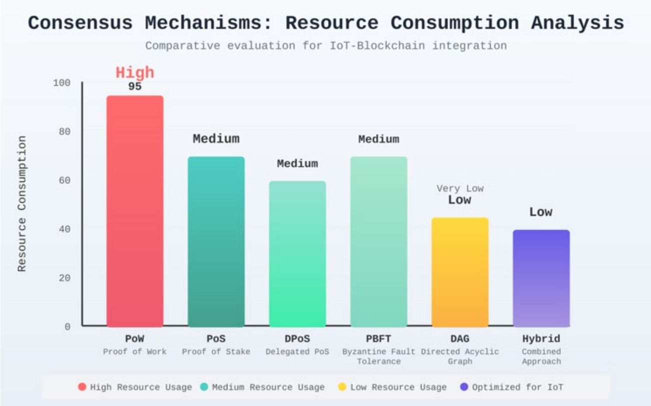


Figure 2. Resource Requirements of Consensus Mechanisms

A more energy efficient approach is Proof of Stake (PoS); however, it creates a different set of difficulties in the IoT environment. The key to this type of selection is large stakes and contributions, which present centralisation dangers to resource-endowed actors [14][19]. The nothing at stake weakness enables validators to vote in a conflicting way without penalty and it may result in forks that undermine trust and destroy security [59]. PoS networks are also vulnerable to long-range attacks, in which one side of the battle gathers stake over time to create historical forks [18]. Although PoS requires less resources than PoW, it is important to consider the resource constraints of the PoS system in detail, especially since different IoT devices can have different connectivity needs [13]. Network token allocation also establishes a new parameter that can lead to unbalanced results of stakeholders in staking [18].

The Delegated Proof of Stake (DPoS) system allows users to elect a small group of delegates who have the responsibility of approving transactions on the network, in a bid to achieve scalability [13]. This method is faster in authentication, making the transactions throughput to increase, which is compatible with Internet of Things (IoT) developments. The authors argue that the weakening of the decentralisation is due to the high network performance that the DPoS has, since the delegates chosen during the selection procedure assume the roles of ensuring the security and reliability of the network [13]. The main trusted risks of the IoT ecosystem include the chances of collusion and elected delegates being compromised. The effectiveness of DPoS in IoT depends on the degree of voter turnout of the token holders, as well as the careful choice of the representatives and the adherence to the integrity standards of the representatives. The integrity and utility of the IoT blockchain can undermine in case voters do not vote or the unqualified delegates are selected. Resource requirements of the implementation of DPoS are significantly less in comparison to Proof of Work (PoW) and different variants of Proof of Stake (PoS); however, when implementing the solutions, it is necessary to consider the limitations of the IoT hardware [21].

Gupta and colleagues present Practical Byzantine Fault Tolerance (PBFT) system, a leader-based consensus system that ensures consensus in blockchain networks even in the case of a malicious or faulty node as a third of the entire amount [44]. The high fault-tolerance level of PBFT is required to ensure high reliability of the IoT systems by ensuring the accuracy and consistency of data processing. It provides high transaction finality, thus making it an efficient way to verify data in applications that require the use of command and validation in real-time [25]. The use of PBFT in the IoT field has a huge disadvantage due to its high communication cost that increases quadratically with the total number of participants [14]. These scalability drawbacks make PBFT inappropriate when it comes to the management of large IoT networks, which are usually constituted of enormous amounts of devices [16]. The leader (primary) node significantly affects the performance and security of PBFT; the vulnerability arises when this node is attacked or lost [25]. Leader election failures create security vulnerabilities that pose a risk to network integrity [24]. According to Gupta in [44], PBFT is best used in permissioned networks, where participants are known and the network has a small number of nodes, whereas the implementation in permissionless IoT networks is faced with challenges as it is difficult to deal with many variable nodes and the protocol is vulnerable to Sybil attacks [24].

The concept of directed acyclic graph (DAG)-based systems is a new alternative to the classical blockchains, and it has significant benefits in terms of the IoT application. DAG structures allow high parallel processing and increased transaction speed because multiple parallel transaction paths are possible to detect, as opposed to using linear sequencing [50]. This architecture is very appropriate to the needs of the large data-processing of IoT devices because it is the parallel processing model. The confirmation of transaction in DAG systems is faster than traditional blockchain and therefore suitable in IoT applications that should validate data in time [30]. Tangle and other platforms that use the DAG model have no transaction fees, which is why they fit the needs of IoT applications that rely heavily on microtransactions [52]. The DAG protocols utilize various approaches to transaction validation and ordering in their platform; however, it is still a complicated task to reach a strong consensus and security [29]. The overall safety of specific DAG-based systems depends on the level of the involvement of participants [31]. The framework of DAG-based techniques has some weaknesses in its relative newness as it was invented later than the existing blockchains, and it can therefore afford less time to prove its security in a wide range of difficult situations [31].

4. Hybrid Consensus Approaches for Blockchain in IoT Applications

Hybrid consensus systems could be seen as a major step forward in the sphere of blockchain engineering because they address such limitations of the conventional consensus protocols that exist when implemented in the context of the Internet of Things (IoT) [15]. These hybrid schemes achieve better performance properties by incorporating two different consensus mechanisms by withstanding high security levels and providing high energy efficiency, scalability and transaction throughput [14].

The combination of the Proof-of-Work (PoW) and Proof-of-Stake (PoS) systems is an example of the hybrid mechanisms that combine the different proof-of-identity mechanism aiming to enhance the efficiency and decrease the power usage [14]. Under the main implementation plan, validation of blocks is done using PoW, meanwhile, PoS is used to perform governance functions and consensus [35]. The architecture combines PoW and PoS to provide a strategy that significantly decreases the energy usage that is traditionally linked to PoW protocols. The PoS element reduces total computational requirements, which increases the viability of certain IoT components hardware. However, hybrid mechanisms should reduce compounding weaknesses and avoid risks of centralization that some PoS systems may suffer and be more energy efficient than traditional PoS systems [37].

As detailed by Routh and Thungon in [27], Practical Byzantine Fault Tolerance (PBFT) is used in conjunction with either PoS or PoW components in hybrid protocols to enhance compatibility of the system with the IoT. Use of PoS in choosing the leader during PBFT rounds contributes to increased fairness and less security vulnerabilities of having a fixed main leader. On the contrary, the combination of PBFT and PoW security infrastructures increases resilience, with the complexity of the PoW solutions meeting the challenging tasks, whereas the PBFT platform enables fast completion of supporting tasks. Yet, there is also a trade-off: because of the high communication overhead of PBFT ($O(n^2)$) the scale of the network is also inherently limited, thus providing a direct trade-off between high-security assurances and the ability to support large-scale IoT deployments. Hierarchical consensus approaches, in turn, offer very specific solutions to the problem of blockchain use in large-scale IoT networks. These mechanisms can support massive scale by organizing the network into a hierarchy of nodes, and support as many as 106 nodes with throughput rates of up to 200800 TPS, as explained in Section 6. The hierarchical model significantly reduces the computational load of the IoT devices through delegation of computational and communication as well as the inclusion of reputation-based systems at every network layer allows authentication facilities that protect the devices within the cluster to enhance overall resilience of IoT systems. Figure 4 illustrates how hierarchical consensus models would be used to resolve the problem of scalability of blockchain in large IoT networks. This is done by the layered system architecture, in which cluster divisions do not interact with each other but they use different consensus mechanisms that are specific to their requirements.

The Figure 3 shows, the Hierarchical Hybrid Consensus Architecture describes the framework of deploying blockchain consensus in IoT scenarios at several levels. According to this design, there are three levels of operation of the various consensus methods, which are determined by the capabilities of the devices and the requirements of a network. The top level of the Global Layer has sensor-armed validator nodes that are deployed in cloud and edge server systems. The following are consensus mechanisms like PoS and PBFT that can be used in these nodes to update the world blockchain state and complete transaction validation. The cluster layer acts as a gateway connecting IoT devices to global validators through the cluster heads that have intermediate computing processing abilities. This layer implements consensus mechanism of DPoS or reputation to aggregate the transactions and pre-verify the transactions and perform a cluster management. The bottom layer consists of the nature of common resource-constrained IoT devices, which accumulate first-time data and simple transactions. The consensus methods at this level are mainly lightweight methods, which make use of a voting mechanism or directed acyclic graph (DAG) to decreasing computational requirements and energy expenses. Information that is emitted by the IoT devices advances to cluster heads and finally to global validators whose resolutions are published across every stratum. An effectively designed system design supports the effective management of resources between devices with different capabilities and security systems of the IoT to provide scalable operations within the limitations of the available IoT resources.

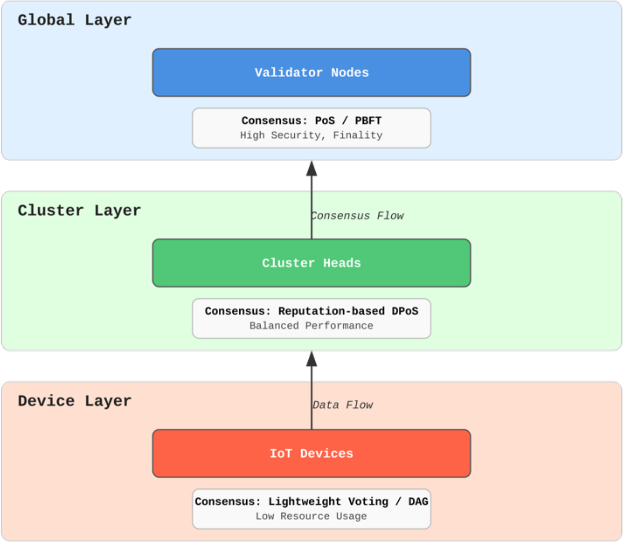


Figure 3. Hierarchical Hybrid Consensus Architecture for IoT environments

The so-called hybrid reputation systems are also a common practice and can be seen as the framework that involves node reputation scores into a consensus mechanism, thus, including the element of trust into the mechanism [14]. In the consensus process, the rating in terms of trustworthy and reliable performance of nodes are used to determine those that have good reputations thus affecting the level of power a node may have in the consensus process or validation of critical blocks. Reputation scoring system acts as a defensive system whereby the network minimizes the participation of nodes that have been found to be unreliable. Reputation score of a node will be promoted by the successful cooperation in the network and compliance with the accepted standards. Combining a reputation-based secure system with PoS or PBFT would provide more flexible, secure consensus mechanisms that are more appropriate in IoT application systems that require a large number of untrusted users.

The time-sensitive hybrid mechanisms required by the urgent hybrid IoT applications, such as Augmented Reality, Virtual Reality, and Industrial IoT, must support very low latency, near-real-time transaction processing. It is a perfectly fit technology to work with industrial automation and autonomous systems [14]. Hybrid consensus protocols refer to different consensus algorithms that have quick finality, including PBFT and voting-based protocols, and methods, including mechanisms, that improve data protection. Transactions are done using fast consensus algorithms on sensor data, and the control commands, and slower, yet more reliable blockchain anchoring algorithms are used periodically. This two needs strategy meets the requirement of speed and security in certain IoT applications. The high efficiency in terms of resource utilization is necessary in order to institute security mechanisms with time-sensitive IoT devices.

5. Case Studies and Implementations in IoT

A range of research has conducted studies on hybrid consensual mechanisms to solve particular issues related to the implementation of blockchain technology in the context of Internet-of-Things (IoT) [69]. The presented case study provides the understanding of what practical advantages and possibilities are related to the application of these approaches. An example of a unique implementation is the use of IOTA as a blockchain that is not structured in a traditional way because it uses a directed acyclic graph (DAG) to generate its ledger [2]. The network is critical in that every new transaction is necessary to verify the previous transactions and create a web of connected transactions. One of the major peculiarities of IOTA is to support micro-transactions as they are likely to be common in many IoT applications [29]. The scalability and transaction throughput of the intake structure can be high because of its capability to process many transactions simultaneously [30]. This means that the more transactions that are introduced to the community, the higher will be the rate of transaction validation [53]. IoT is not using a proof-of-work as a primary consensual mechanism, and instead it is used to discourage unsolicited and illicit transactions [29]. IOTA platform has been explored with a number of uses in IoT applications... It is a DAG-based network, the Tangle, designed to be highly scaled and transaction throughput and achieves 800-1000^{-} TPS over networks of up to 106 nodes with a low power cost of 10-25W. This renders it specifically applicable to IoTs with high micro-transactions and energy-limited power options [54].

The Roll-Delegated Proof-of-Stake (DPoS) consensus mechanism is among the Internet of Things (IoT) consensus mechanisms developed by IoTeX and made to achieve scalability and efficiency in IoT settings [60]. Through this system, the randomly selected delegated Proof-of-Stake is used, according to which a certain number of representatives is randomly selected to create new blocks [63]. A community voting system is used in the process of selecting a set of validator nodes [61]. IoTeX has got an EVM-compatible blockchain, which allows using smart contracts [62]. The mission is to have self-sovereign IoT devices and applications that are interested in user privacy and data management [60]. To solve the problems of scalability and decentralization that occur when traditional DPoS is extended to a large, heterogeneous resource system like IoT, Roll-DPoS introduces a more flexible and less predictable block-producer selection mechanism [61]. Hyperledger Fabric is a permissioned blockchain architecture that is designed with enterprise-level IoT applications that demand high privacy and access-control [10]. Fine-grained access, privacy, and organisational policies Advanced controls: Protection from many industrial IoT applications require controls which are fine-grained to achieve privacy and organisational policies [66]. The system has pluggable consensus mechanisms, which allows organisations to adjust their blockchain operations to it [65]. The extension is applied to protect data collection, storage, and sharing in different IoT settings, which results in an increase in security, efficiency, and the total system capacity [64]. It has been shown that it can be optimised to reach high transaction throughput, especially with certain optimisations [67].

Also, one of the most important uses of the hybrid consensus approach to blockchain is the reputation-based hybrid consensus mechanism (HCM) applied to electronic healthcare systems (EHS) [33]. It is an HCM that uses a mixture of algorithms, to create, to validate, handle forks, build Merkle trees and a reward/punishment module, all positioned on the observed activities of the different blocks within the system. Another framework is the H-chain framework, which is specifically aimed at IoT ecosystems that consist of a number of collaborating organisations [34]. Routh and Thungon [27] suggested a hybrid blockchain using Practical Byzantine Fault Tolerance (PBFT) instances of a private blockchain coupled with a public blockchain based on permissioned Proof of Work (PoW) consensus mechanism. The design should be the balance between the needs to ensure the check of such transactions privately and to have information that can be audited publicly. This is a consensus algorithm that is suggested to implement in IoT applications based on blockchain, which upgrades scalability by means of election of master-node and limited broadcast domain, which makes it suitable to resource-limited IoT devices [29]. Microchain introduces the high-level architecture of a lightweight hierarchical consensus protocol in the IoT optimized with Proof of Concept (PoC) and Voting-based Chain Finality (VCF) consensus protocol [55] to produce blocks. The current paper introduces a hierarchical and location-aware consensus protocol, which is abbreviated LH-Raft, aimed at IoT-blockchain applications. It forms local consensus groups founded on reputation and local information of nodes, thus increasing the network scalability and decreasing the expenses of communications [57, 58]. This difference in implementations highlights the ongoing research and development of the field of hybrid consensus mechanisms, which are customized to the needs and limitations of different domains of IoT usage, including sensitive healthcare data management and large-scale industrial control systems [36].

6. Performance Analysis and Comparison

The performance of hybrid consensus mechanisms in the applications of the IoT needs a comprehensive framework based on different performance metrics. The main features are energy-efficiency, which is essential to resource-constrained IoT devices, scalability, which is the ability to serve many devices and large volumes of transactions; transaction throughput, the number of transactions verified per second; security guarantees, the ability to resist many attacks common in an IoT system; fault tolerance, the ability to withstand several device failures or malicious activities; and abilities related to a latency, which means the time that a transaction needs to be confirmed and integrated into the blockchain [56]. Both options have trade-offs as explained in a study of many hybrid consensus mechanisms in the light of these important metrics. Other design versions, including PoW/PoS hybrids, are of medium energy efficiency, medium scalability, and transaction throughput, and of high to medium security assurance and fault tolerance. These systems are either probabilistic (PoW based) or stake based (PoS based), and medium-high latency. PBFT based on PoS or PoW functionality has moderate energy efficiency and scalability, medium throughput and high throughput, and high security and fault tolerance and low or medium latency [28]. Generally, hierarchical consensus models are medium to high energy efficient, medium to high throughput, medium to high security, and fault tolerant, and vary in layer-dependent medium to high energy efficiency, and medium to low latency. The reputation based hybrids have medium to high energy efficiency, scaling, and medium to high throughput. Their other advantages include better security and fault tolerance because of the reputation system, and the latency is medium to low. Hybrids, which are time sensitive, offer low latency with high throughput and medium energy efficiency and scalability. Depending on the combination of mechanisms used security and fault tolerance differ. The hierarchical consensus models normally offer medium to high energy efficiency and small scalability features with medium to high throughput. Depending on the layer implementation, their security and fault tolerance are medium to low latency. Reputation-based hybrids are generally characterized by desirable energy efficiency and scalability, medium to high throughput and enhanced security and fault tolerance due to their reputation systems, and medium to low latency. Hybrids that are time-sensitive focus on low latency and high throughput, with medium energy efficiency and scalability, and security and fault tolerance depending on the mechanisms used.

The IOTA Tangle (based on DAG) is designed to be more energy efficient, scalable, and throughput. Their security is based on network activity, and fault tolerance of the DAG structure that leads to low latency. TheRoll-DPoS by IoTeX aims to improve the energy-efficiency, scalability, and throughput by the use of stake-based security, and delegate-based fault tolerance, which, in turn, leads to low latency [60]. Hyperledger Fabric has adjustable consensus mechanisms that have performance characteristics. It usually offers medium scalability, high throughput, and permissioned network security, as well as, adjustable fault tolerance and low latency. The reputation-based HCM has average energy efficiency, scaling, throughput, as well as better security and fault tolerance with its reputation module, in addition to medium latency. The H chain combines Proof of Work (PoW) and Practical Byzantine Fault Tolerance (PBFT), which show adjustable energy usage and mediocre scalability, medium throughput, high security and fault tolerance, and mediocre latency. CBCIoT which is a voting based mechanism is highly energy efficient, scalable and has through put, rating based security, majority based fault tolerance as well as low latency. Table 2 shows the summary of the performance comparison across different hybrid consensus mechanisms of IoT.

Table 2. Comparative Positioning with Recent Survey Literature

Mechanism	Energy (mW)	Max Nodes	Throughput (TPS)	Latency (sec)	Security Model	Fault Tolerance
PoW/ PoS Hybrid	45 to 60	10^3 to 10^4	50-150	3-8	51% attack resistant	Probabilistic
PBFT +PoS/ PoW	30 to 50	10^2 to 10^3	100-300	1-4	Byzantine resilient	f < n/3
Hierarchical	15 to 60	10^4 to 10^6	200-800	2-6	Layer-dependent	Multi-level
Reputation-based	20 to 40	10^3 to 10^5	150-500	2-5	Trust-based	Adaptive
Time-sensitive	25 to 45	10^3 to 10^4	500-1500	0.5-2	Variable	Real-time

IOTA Tangle	10 to 25	10^5 to 10^6	800-1000	1-3	Network-dependent	DAG structure
IoTeX Roll-DPoS	20 to 35	10^4 to 10^5	500-1000	1-2	Stake-weighted	Delegate-based
Hyperledger Fabric	30 to 55	10^2 to 10^4	500-3500	0.5-3	Permissioned	Configurable

Note: Performance ranges compiled from implementation studies and experimental analyses reported in references [12, 18, 33, 34, 52, 60, 64, 67]. Values represent typical operational characteristics under standard IoT workloads. Actual performance varies with specific implementation parameters and network conditions.

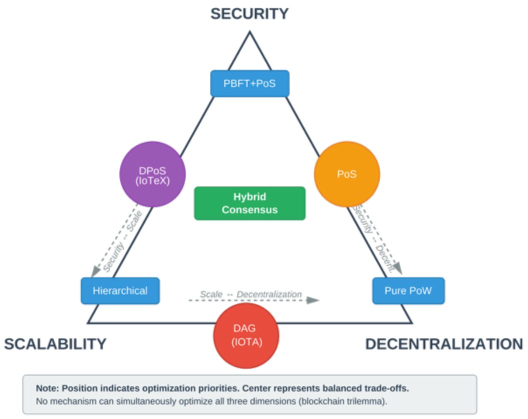
The effectiveness of hybrid consensus mechanisms in the IoT has a significant impact on the combination of algorithms and network architecture, and characteristics of IoT devices. This lack of a universal solution dictates that the choice of the most appropriate mechanism lies in carefully considering the peculiarities of the application's needs and limitations within the context of its use. Considering constraints such as energy, scalability, security, and latency tolerance is crucial in determining the most suitable hybrid consensus for a specific Internet of Things application.

6.1 Trade-off Analysis Framework

The quantitative comparison in Table 1 synthesizes performance characteristics from documented implementations and experimental studies. Energy consumption values represent operational power requirements for IoT gateway devices participating in consensus, with DAG-based approaches (IOTA) demonstrating the lowest consumption and PoW hybrids the highest. Scalability metrics indicate maximum network sizes tested in implementation studies, ranging from hundreds of nodes for PBFT variants to millions for hierarchical and DAG architectures. Transaction throughput measured in transactions per second (TPS) varies significantly, with time-sensitive mechanisms and enterprise frameworks (Hyperledger Fabric) achieving the highest rates. Latency represents average transaction confirmation time, critical for real-time IoT applications. These metrics reveal fundamental trade-offs: mechanisms optimizing for security and fault tolerance (PBFT variants) sacrifice scalability and energy efficiency, while highly scalable approaches (DAG-based, hierarchical) accept reduced decentralization or network-activity-dependent security. Mechanism selection must therefore align with specific application priorities—healthcare systems prioritizing security over scalability, smart cities requiring extreme scale with acceptable energy costs, and industrial automation demanding low latency above all else.

6.2 Trade-off Analysis Framework

Hybrid consensus mechanisms for IoT applications confront fundamental trade-offs among three competing objectives: security, scalability, and decentralization—collectively referred to as the "blockchain trilemma." Unlike cryptocurrency applications, where this trilemma represents theoretical optimization challenges, IoT deployments face hard constraints imposed by device capabilities and application requirements. Understanding these trade-offs is crucial for selecting mechanisms aligned with specific IoT scenarios. Figure 5 provides a visual synthesis of these trade-offs, positioning various mechanisms within the security-scalability-decentralization space.



Note: Position indicates optimization priorities. Center represents balanced trade-offs.
No mechanism can simultaneously optimize all three dimensions (blockchain trilemma).

Figure 5. The blockchain trilemma in IoT contexts. Hybrid consensus mechanisms position themselves strategically within this trade-off space based on application priorities, with no single mechanism optimizing all three dimensions simultaneously.

Security-Scalability Trade-off: High-security mechanisms employing Byzantine fault tolerance (PBFT variants) or proof-of-work components inherently limit scalability. PBFT's communication complexity scales quadratically with participant count ($O(n^2)$), restricting practical deployments to hundreds or low thousands of nodes despite providing deterministic finality and 33% Byzantine fault tolerance. Healthcare IoT applications prioritize this trade-off, accepting limited network scale to ensure cryptographic guarantees for sensitive patient data. Conversely, hierarchical consensus architectures achieve scalability exceeding 10^6 nodes by fragmenting the network into clusters with localized consensus, necessarily reducing global decentralization as cluster heads become trust concentrations. Smart city deployments spanning millions of sensors accept this centralization to achieve operational feasibility.

Scalability-Decentralization Trade-off: Mechanisms achieving extreme scalability typically sacrifice decentralization through delegation or hierarchical structures. IoTeX's Roll-DPoS demonstrates this compromise: randomly selected delegates enable high throughput (500-1000 TPS) and support for 10^4-10^5 nodes, yet consensus authority concentrates among validator delegates rather than distributing across all participants. Similarly, hierarchical architectures introduce trust assumptions at cluster head and validator layers. This trade-off proves acceptable for industrial IoT where operational efficiency supersedes ideological decentralization, but problematic for applications requiring trustless operation across organizational boundaries.

Security-Energy Trade-off: Energy-constrained IoT devices cannot support computationally intensive security mechanisms. Proof-of-work components, while providing robust Sybil resistance, consume 45-60 mW—prohibitive for battery-powered sensors requiring multi-year operation. DAG-based approaches (IOTA Tangle) minimize energy consumption (10-25 mW) through lightweight proof-of-work solely for spam prevention, accepting network-activity-dependent security where low transaction volumes increase vulnerability to attacks. Wearable health monitors and environmental sensors prioritize energy efficiency, tolerating reduced security guarantees achievable within power budgets below 30 mW.

6.1.1 Application-Specific Optimization Strategies

Optimal mechanism selection requires explicit prioritization of constraints:

Critical Infrastructure (Healthcare, Financial): Security > Latency > Energy > Scalability. Deploy PBFT+PoS hybrids accepting limited scale (10^3 nodes) and moderate energy consumption (30-50 mW) for deterministic Byzantine fault tolerance and cryptographic finality guarantees.

Large-Scale Monitoring (Smart Cities, Agriculture): Scalability > Energy > Throughput > Security. Implement hierarchical consensus enabling 10^5-10^6 nodes with layered trust models, accepting centralization at aggregation points while maintaining lightweight device-layer protocols (15-35 mW).

Real-Time Control (Industrial Automation, Autonomous Vehicles): Latency > Throughput > Security > Scalability. Utilize time-sensitive hybrids achieving sub-second confirmation (0.5-2 sec) and high throughput (500-1500 TPS), balancing moderate energy consumption (25-45 mW) against application-specific security requirements.

Energy-Constrained Networks (Wireless Sensors, Wearables): Energy > Latency > Scalability > Security. Adopt DAG-based or lightweight voting mechanisms operating below 30 mW, accepting security dependencies on network activity and reduced decentralization.

Hybrid Mechanisms as Trade-off Optimization: The fundamental value proposition of hybrid consensus lies not in eliminating the blockchain trilemma but in providing tunable parameters to optimize for specific constraint profiles. By combining complementary mechanisms—PBFT for finality with PoS for fairness, hierarchical structures for scale with reputation systems for trust—hybrid approaches enable application-specific positioning within the security-scalability-decentralization design space. However, this flexibility introduces complexity: each additional mechanism component expands the attack surface and complicates formal security analysis, as demonstrated by vulnerabilities emerging from unexpected interactions between consensus layers in hierarchical systems. No universal optimal hybrid consensus exists for IoT applications. The mechanisms compared in Table 2 represent different points in the trade-off space, each suitable for distinct application scenarios. Practitioners must conduct explicit constraint analysis—quantifying energy budgets, scalability requirements, latency tolerance, and security threat models—before selecting mechanisms, recognizing that gains in one dimension necessarily impose costs in others.

7. Open Challenges and Future Directions

Important issues remain because current developments of hybrid consensus protocols to blockchain technology, especially in the field of the IoT, have revealed various unresolved problems that require the attention of scholars. One of the most critical challenges is the need to standardize agreement between hybrid systems, which will help to implement them on a large scale and interact at the level of IoT [47]. The absence of standardized or protocol between the varying versions makes integration difficult and this may prevent the reusability of solutions that were provided by other software vendors. This therefore necessitates standardization of interfaces, data formats and security requirements in Internet of Things (IoT) consensus hybrids. Lack of internationally established standards fosters disintegration, thus halting investments in individual solutions as a result of vendor lock-in. This interoperability is therefore limited and limits the possibility of breakthroughs. Another prominent issue is one to ensure seam inter-protocol connections in a hybrid architecture [14]. Even though such mechanisms like PoW or PBFT are well known, their interplay may introduce unexpected, second-order attack vectors; e.g. a weakness in a PoS-based leader election during a round of the PBFT may discredit the integrity of the system. Such multi-protocol systems have therefore become a significant and unresolved area of research that needs formal verification. The vulnerabilities to a blockchain-based system design of an IoT system can be reduced through a thorough security evaluation and rigorous testing to comprehensively build a robust system design. Similarly, the interactions between the many consensus components shall be properly studied to ensure that the system is not observed to have reduced strength compared to the constituents. Major issues of scalability persist especially in massive IoT systems that involve billions of devices and extreme transaction volumes [13]. Although there are not many mixed systems that can exhibit better scalability with regard to the traditional mechanisms, large volumes of research and development are required to make the mixed systems change and adapt to meet the requirements of a large IoT system with its issue of limited and low-latency information processing. Scalability of blockchain-based IoT solutions utilizing hybrid mechanisms of consensus is a developing field of research.

However, there are certain opportunities and threats of this landscape. Switching to architectures with distributed processing would help increase the efficiency and scalability of hybrid consensus, which has been difficult to target. This kind of transition imperatively requires the solution of the problem of data consistency, security, and synchronization between the heterogeneous layers of heterogeneous distributed environments [68]. Facilitating a smooth and safe interfacing between blockchain layer and distributed computing architectures is a complicated issue. The regulatory capacity of incorporating blockchain and IoT is becoming increasingly important, including hybrid consensus mechanisms [5]. The existing and possible regulatory frameworks of data privacy, security, and governance should be considered necessary. The possibility to adhere to regulations including GDPR, which grants users with the option to amend or destroy their information, is rather challenging because blockchain records cannot be changed [24]. The use of hybrid mechanisms can thus entail the need to include the elements of enforcement that would meet those requirements without compromising the primary benefits of blockchain technology [48].

8. Conclusion

The introduction of blockchain technology into an Internet of Things can bring considerable opportunities to the improvement of security of interconnected systems that are more and more susceptible to breaches and data manipulation. Although there are a lot of traditional consensus mechanisms suggested to use in blockchain, none of them have been efficient in meeting the particular needs of IoT. This situation can change with the introduction of hybrid consensus approaches. These mechanisms are strategic to combine the advantages of different consensus protocols in balancing energy and scalability, throughput and security and fault tolerance, and latency, to meet the different needs of diverse IoT applications. Hybrid consensus mechanisms landscape includes many different models, including PoW/ PoS hybrids, PBFT with PoS or PoW components, hierarchical consensus models, reputation based models and time sensitive hybrid mechanisms. Examples of apps such as IOTA - Tangle, IoTeX - Roll-DPoS, and Hyperledger Fabric that are used to work with the IoT represent innovation in various fields. Comparative analysis of the performance has brought to the fore the trade-offs of each method, to point to the fact that the performance results can differ dramatically depending on the requirements of the particular IoT application. Even though progress has been made, there are still a number of questions that are unanswered. The problem of compatibility requirements remains hindrance to intercommunication and the drawbacks of complex hybrid designs are worth in-depth investigation. Issues related to scalability in large scale IoT deployments, compatibility with new IoT standards, and responsiveness to a changing legal environment are still unaddressed. Future studies need to focus on establishing common paradigms of hybrid consensus in IoT, which are supported by extensive security studies of ongoing and innovative procedures. In addition, it should work towards scalability of ultra -scale IoT networks, guarantee a seamless interface with edge and fog computing models, and develop blockchain solutions that align with the IoT. Practitioners need to provide an extensive analysis of the unique needs that are relevant to their IoT applications. When choosing a suitable hybrid consensus mechanism, factors like resource constraints of a device, the kind of data required to be processed and stored and, possibly, security needs should be taken into consideration. The analysis of the performance trade-offs related to the existing performance with regard to the integration of blockchain technology requires a specific analysis of the performance trade-offs. The open problems, whether of varying perspectives or of lack of resources to deal with them, are problems that require an in-depth analysis which is commensurate with the level of knowledge one has in the field.

Declarations

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

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

References

[1] Pal S, Hitchens M, Rabehaja TM, Mukhopadhyay SC. Security requirements for the Internet of Things: a systematic approach. Sensors (Basel). 2020;20(20):5897. doi: 10.3390/S20205897

[2] Alhavan M, Azimi A, Corchado JM. A CoviReader architecture based on IOTA Tangle for outbreak control in smart cities during COVID-19 pandemic. Med J Islam Repub Iran. 2022;36:180. doi: 10.47176/mjiri.36.180

[3] Dirin A, Oliver I, Laine TH. A security framework for increasing data and device integrity in Internet of Things systems. Sensors (Basel). 2023;23(17):7532. doi: 10.3390/s23177532

[4] Anosike CN, Adeleke OJ, Adediji AP, Okereke RO, Cynthia UC, Sodipe AO. Review of IoT device security, methods to enhance security and prevent cyber attacks and data breaches. Authorea. 2024 Aug 28. doi: 10.22541/au.172481288.88002325/v1

[5] Zorrilla M, Yebenes J. A reference framework for the implementation of data governance systems for industry 4.0. Comput Stand Interfaces. 2022;81:103595. doi: 10.1016/j.csi.2021.103595

[6] Sulaeman AA. Blockchain-powered security framework for IoT data integrity and privacy. J Acad Sci. 2025;2(3):874-882.

[7] Oh T. Blockchain-enabled security enhancement for IoT networks: integrating LEACH algorithm and distributed ledger technology. J Mach Comput. 2025:483–495. doi: 10.53759/7669/jmc202505038

[8] Verma R, Thakur S, Vaidya P, Sharma BB. Blockchain-enabled IoT: revolutionizing security and data integrity in connected devices. In: 2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON). IEEE; 2024. p. 1-5.

[9] Almarri S, Aljughaiman A. Blockchain technology for IoT security and trust: a comprehensive SLR. Sustainability. 2024;16(23):10177. doi: 10.3390/su162310177

[10] Alkurdi F, Elgendi I, Munasinghe KS, Sharma D, Jamalipour A. Blockchain in IoT security: a survey. In: 2018 28th International Telecommunication Networks and Applications Conference (ITNAC). IEEE; 2018. p. 1-4.

[11] Ahakonye LAC, Nwakanma CI, Kim DS. Tides of blockchain in IoT cybersecurity. Sensors (Basel). 2024;24(10):3111. doi: 10.3390/s24103111

[12] Vavilis S, Niavis H, Loupos K. A fair and lightweight consensus algorithm for IoT. arXiv preprint arXiv:2503.08607. 2025.

[13] Ragul M, Aloysius A, Kumar VA. Enhancing IoT blockchain scalability through the eepos consensus algorithm. Sci Temper. 2025;16(1):3698–3709. doi: 10.58414/SCIENTIFICTEMPER.2025.16.1.16

[14] Zhuang Y, Chen Y, Zhang X, Ren T, Han M, Alam M, et al. A large-scale node lightweight consensus algorithm of blockchain for Internet of Things. IEEE Internet Things J. 2024.

[15] Bommireddy NR. Consensus for creating light weight blockchain for IoT [Dissertation]. Southern Illinois University at Carbondale; 2024.

[16] Haque EU, Abbasi W, Almogren A, Choi J, Altameem A, Rehman AU, et al. Performance enhancement in blockchain based IoT data sharing using lightweight consensus algorithm. Sci Rep. 2024;14(1):26561. doi: 10.1038/s41598-024-77706-x

[17] Hsueh C-W, Chin C-T. Toward trusted IoT by general proof-of-work. Sensors (Basel). 2023;23(1):15. doi: 10.3390/s23010015

[18] Lepore C, Ceria M, Visconti A, Rao UP, Shah KA, Zanolini L. A survey on blockchain consensus with a performance comparison of PoW, PoS and pure PoS. Mathematics. 2020;8(10):1782.

[19] Nguyen CT, Hoang DT, Nguyen DN, Niyato D, Nguyen HT, Dutkiewicz E. Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access. 2019;7:85727-85745.

[20] Khan M, den Hartog F, Hu J. A survey and ontology of blockchain consensus algorithms for resource-constrained IoT systems. Sensors (Basel). 2022;22(21):8188. doi: 10.3390/s22218188

[21] Sapra N, Shaikh I, Dash A. Impact of proof of work (PoW)-based blockchain applications on the environment: a systematic review and research agenda. J Risk Financ Manag. 2023;16(4):218.

[22] Amin MR. 51% attacks on blockchain: a solution architecture for blockchain to secure iot with proof of work [Bachelor Thesis]. Dhaka, Bangladesh: International University of Business Agriculture and Technology; 2020.

[23] Parmar M, Kaur HJ. Blockchain-enabled consensus routing protocol improving the security data communication in Internet of Things applications. Int J Comput Netw Appl. 2021;8(4):268-276.

[24] Liu S, Zhang R, Liu C, Xu C, Wang J. An improved PBFT consensus algorithm based on grouping and credit grading. Sci Rep. 2023;13(1):13030. doi: 10.1038/s41598-023-28856-x

[25] Qi J, Guan Y. Practical Byzantine fault tolerance consensus based on comprehensive reputation. Peer-to-Peer Netw Appl. 2023;16(1):420-430.

[26] Yuan F, Huang X, Zheng L, Wang L, Wang Y, Yan X, et al. The evolution and optimization strategies of a PBFT consensus algorithm for consortium blockchains. Information. 2025;16(4):268. doi: 10.3390/info16040268

[27] Routh A, Thungon LC. IoTSecChain: advancing IoT network communications with PBFT consensus and ECC authentication. Authorea. 2024 Nov 20. doi: 10.22541/au.173210446.67966051/v1

[28] Singh R, Nandi S. An improved pbft-based consensus protocol for industrial iot. In: 2023 IEEE/ACM 23rd

International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW). IEEE; 2023. p. 311-312.
[29] Uddin M, Muzammal M, Hameed MK, Javed IT, Alamri B, Crespi N. CBCIoT: a consensus algorithm for blockchain-based IoT applications. Appl Sci. 2021;11(22):11011.
[30] Raikwar M, Polyanskii N, Müller S. SoK: DAG-based consensus protocols. In: 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE; 2024. p. 1-18.
[31] Pervez H, Muneeb M, Irfan MU, Haq IU. A comparative analysis of DAG-based blockchain architectures. In: 2018 12th International conference on open source systems and technologies (ICOSST). IEEE; 2018. p. 27-34.
[32] de Morais AM, Lins FAA, Rosa NS. Survey on integration of consensus mechanisms in IoT-based blockchains. J Univers Comput Sci. 2023;29(10):1139.
[33] Prabha P, Chatterjee K. Design and implementation of hybrid consensus mechanism for IoT based healthcare system security. Int J Inf Technol. 2022;14(3):1381-1396.
[34] Hu J, Reed MJ, Al-Naday M, Thomos N. Hybrid blockchain for IoT—energy analysis and reward plan. Sensors (Basel). 2021;21(1):305.
[35] Aggarwal S, Kumar N. Cryptographic consensus mechanisms. In: Advances in computers. Vol. 121. Elsevier; 2021. p. 211-226.
[36] Kumari T, Kumar R, Dwivedi RK. Blockchain-based secure and smart healthcare iot system using hybrid consensus mechanism with an honest block. Health Serv Outcomes Res Methodol. 2025;25(1):113-151.
[37] Alkhateeb A, Catal C, Kar G, Mishra A. Hybrid blockchain platforms for the internet of things (IoT): a systematic literature review. Sensors (Basel). 2022;22(4):1304.
[38] Wingreen SC, Kavanagh D, Dylan-Ennis P, Miscione G. Sources of cryptocurrency value systems: the case of Bitcoin. Int J Electron Commer. 2020;24(4):474-496.
[39] Tanwar S. Blockchain technology. In: Blockchain Regulation and Governance in Europe. 2018.
[40] Jaradat A, Ali O, AlAhmad A. Blockchain technology: a fundamental overview. In: Blockchain technologies for sustainability. Singapore: Springer Singapore; 2021. p. 1-24.
[41] IBM. What Is Blockchain? [Internet]. 2021. Available from: https://www.ibm.com/think/topics/blockchain
[42] Black Duck. What Is Blockchain and How Does It Work? [Internet]. 2025. Available from: https://www.blackduck.com/glossary/what-is-blockchain.html
[43] Eze KG, Akujuobi CM, Sadiku MN, Chouikha M, Alam S. Internet of things and blockchain integration: use cases and implementation challenges. In: Business Information Systems Workshops: BIS 2019 International Workshops. Springer International Publishing; 2019. p. 287-298.
[44] Gupta S, Hellings J, Rahnama S, Sadoghi M. An in-depth look of BFT consensus in blockchain: challenges and opportunities. In: Proceedings of the 20th international middleware conference tutorials; 2019. p. 6-10.
[45] Kim H, Kim D. A taxonomic hierarchy of blockchain consensus algorithms: an evolutionary phylogeny approach. Sensors (Basel). 2023;23(5):2739.
[46] Makhdoom I, Abolhasan M, Abbas H, Ni W. Blockchain's adoption in IoT: the challenges, and a way forward. J Netw Comput Appl. 2019;125:251-279.
[47] George I. Exploring the integration of blockchain in IoT use cases: challenges and opportunities. 2024.
[48] Atlam HF, Alenezi A, Alassafi MO, Wills G. Blockchain with internet of things: benefits, challenges, and future directions. Int J Intell Syst Appl. 2018;10(6):40-48.
[49] Obaidat MA, Rawashdeh M, Alja'afreh M, Abouali M, Thakur K, Karime A. Exploring IoT and blockchain: a comprehensive survey on security, integration strategies, applications and future research directions. Big Data Cogn Comput. 2024;8(12):174.
[50] Qu X, Wang S, Li K, Huang J, Cheng X. TidyBlock: a novel consensus mechanism for DAG-based blockchain in IoT. IEEE Trans Mob Comput. 2024.
[51] Khan M, Hartog FD, Hu J. Toward verification of DAG-based distributed ledger technologies through discrete-event simulation. Sensors (Basel). 2024;24(5):1583.
[52] Sealey N, Aijaz A, Holden B. IOTA tangle 2.0: toward a scalable, decentralized, smart, and autonomous IoT ecosystem. In: 2022 International Conference on Smart Applications, Communications and Networking (SmartNets). IEEE; 2022. p. 01-08.
[53] Ahuja S, Johari R, Khokhar C. IoTA: Internet of things application. In: Proceedings of the Second International Conference on Computer and Communication Technologies: IC3T 2015. New Delhi: Springer India; 2015. p. 235-247.
[54] Pullo S, Pareschi R, Piantadosi V, Salzano F, Carlini R. Integrating iota's tangle with the internet of things for sustainable agriculture: a proof-of-concept study on rice cultivation. Informatics. 2023;11(1):3.
[55] Xu R, Chen Y, Blasch E. Microchain: a light hierarchical consensus protocol for iot systems. In: Blockchain Applications in IoT Ecosystem. Cham: Springer International Publishing; 2020. p. 129-149.
[56] Al Ahmed MT, Hashim F, Hashim SJ, Abdullah A. Hierarchical blockchain structure for node authentication in IoT networks. Egypt Inform J. 2022;23(2):345-361.
[57] Guo H, Li W, Nejad M. A hierarchical and location-aware consensus protocol for IoT-blockchain applications. IEEE Trans Netw Serv Manag. 2022;19(3):2972-2986.

[58] Guo H, Li W, Nejad M. A location-based and hierarchical framework for fast consensus in blockchain networks. In: 2021 4th International Conference on Hot Information-Centric Networking (HotICN). IEEE; 2021. p. 1-6.

[59] Ramírez-Gordillo T, Maciá-Lillo A, Pujol FA, García-D'Urso N, Azorín-López J, Mora H. Decentralized identity management for Internet of Things (IoT) devices using IOTA blockchain technology. Future Internet. 2025;17(1):49.

[60] Coinbase. IoTeX Price, IOTX Price, Live Charts, and Marketcap [Internet]. [cited 2024 Nov 21]. Available from: https://www.coinbase.com/price/iotex

[61] Chai R, Guo Q, Sun J, Fan X. An Overview of IOTEX (Iotx) [Internet]. Pontem Network; [cited 2025 Mar 28]. Available from: https://pontem.network/posts/an-overview-of-iotex-iotx

[62] The report by Messari on the IoTex platform update: the DePIN sector advances. The Cryptonomist [Internet]. 2024 Nov 18. Available from: 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. 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; 2018. p. 482-484.

[64] Honar Pajooh H, Rashid M, Alam F, Demidenko S. Hyperledger fabric blockchain for securing the edge internet of things. Sensors (Basel). 2021;21(2):359.

[65] IBM. What Is Hyperledger Fabric? [Internet]. 2021 Jul 16. Available from: https://www.ibm.com/think/topics/hyperledger

[66] Jarwar MA, Ali S, Shah SC. Taking IoT security to the next level: Hyperledger fabric private blockchain enabled IoT middleware. In: 2023 IEEE Globecom Workshops (GC Wkshps). IEEE; 2023. p. 1325-1330.

[67] Honar Pajooh H, Rashid MA, Alam F, Demidenko S. Experimental performance analysis of a scalable distributed hyperledger fabric for a large-scale IoT testbed. Sensors (Basel). 2022;22(13):4868.

[68] Abdulrahman E, Alshehri S, Alzubaidy A, Cherif A. A distributed blockchain-based access control for the Internet of Things. arXiv preprint arXiv:2503.17873. 2025.

[69] Barrera D, Bellman C, Van Oorschot P. Security best practices: a critical analysis using IoT as a case study. ACM Trans Priv Secur. 2023;26(2):1-30.

[70] Sharma A, Babu LG, Buradkar MU, Shanmathi M, Vinisha J, Udhayamoorthi M. Integration of blockchain and IoT for enhanced transparency in diamond supply chain. EAI Endorsed Trans Internet Things. 2025;11. doi: 10.4108/eetiot.7145

[71] Abbasi M, Prieto J, Plaza-Hernandez M, Corchado JM. Proof-of-resource: a resource-efficient consensus mechanism for IoT devices in blockchain networks. EAI Endorsed Trans Internet Things. 2024;10. doi: 10.4108/eetiot.6565