Internet of Things 36 (2026) 101872

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Review article

Bibliometric analysis of secure IoT for quantum computing

Hamza Ibrahim [a], Love Allen Chijioke Ahakonye [b], Jae-Min Lee [a], Dong-Seong Kim [a,c,*]

[a] IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, 39177, South Korea
[b] NSLab Co. Ltd., Kumoh National Institute of Technology, Gumi, 39177, South Korea
[c] ICT-Convergence Research Center, Kumoh National Institute of Technology, Gumi, 39177, South Korea

ARTICLE INFO

Keywords:
6G networks
Blockchain
Industrial IoT
Quantum Machine Learning
Bibliometric analysis
Network security

ABSTRACT

The convergence of Quantum Machine Learning (QML) and Blockchain is emerging as a transformative paradigm to address escalating security and scalability challenges in 6G-enabled Industrial Internet of Things (IIoT) networks. This study presents the first comprehensive bibliometric and meta-analysis of this nascent interdisciplinary field. We analyzed 159 peer-reviewed publications (indexed from January 2022 through December 22, 2024) from Scopus, employing a systematic Kitchenham-based methodology for literature selection and VOSviewer for science mapping. Our analysis reveals a 75% annual growth rate since 2022, with India (37.7%), the USA (12.6%), and South Korea (12.6%) as the leading contributors. Keyword co-occurrence analysis identified four dominant thematic clusters: “6G Network Security," “Quantum Computing and AI," “Blockchain and Decentralization," and “IIoT Applications." The study’s novelty lies in synthesizing bibliometric insights with a proposed five-layer QML-Blockchain integration framework and a comparative analysis against existing reviews. Quantitative performance metrics indicate that QML can improve anomaly detection accuracy by 5–9% over classical models, while advanced consensus mechanisms like PoA^2 can reduce transaction latency by 35%. However, significant challenges persist, including quantum hardware limitations (e.g., qubit coherence <100 μs), scalability challenges in achieving consensus across massive IIoT device densities, and a critical lack of empirical testbeds. This research provides a foundational roadmap, emphasizing the urgent need for standardized benchmarks, hybrid orchestration models, and quantum-resistant cryptography to realize secure, intelligent, and autonomous IIoT ecosystems in the 6G era.

1. Introduction

The Industrial Internet of Things (IIoT) represents a pivotal advancement in industrial automation, enabling unprecedented connectivity, data exchange, and operational intelligence across critical sectors such as manufacturing, energy, and healthcare [1,2]. The imminent transition to 6G networks promises to further revolutionize this landscape through ultra-reliable low-latency communication (URLLC), pervasive artificial intelligence (AI), and terahertz-speed connectivity [3]. However, this evolution also expands the attack surface, introducing novel security vulnerabilities and escalating computational demands on conventional cryptographic and machine learning frameworks [4].

Two disruptive technologies have garnered significant research interest in response: Quantum Machine Learning (QML) and Blockchain. QML leverages fundamental quantum principles, superposition and entanglement, to potentially achieve exponential

* Corresponding author.
E-mail addresses: loveahakonye@kumoh.ac.kr (L.A.C. Ahakonye), ljmpaul@kumoh.ac.kr (J.-M. Lee), dskim@kumoh.ac.kr (D.-S. Kim).

https://doi.org/10.1016/j.iot.2026.101872
Received 16 October 2025; Received in revised form 4 January 2026; Accepted 14 January 2026
Available online 16 January 2026
2542-6605/

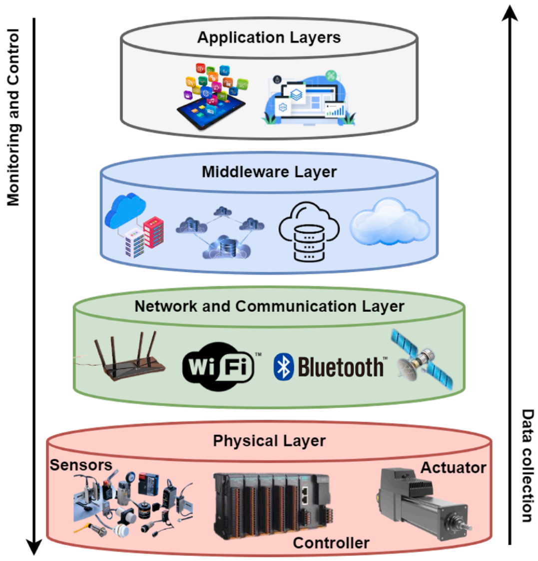

Figure 1. IIoT architectural layers.

speedups in complex optimization and pattern recognition tasks critical for IIoT, such as real-time anomaly detection and predictive maintenance [5,6]. Concurrently, Blockchain technology offers a decentralized trust model, ensuring data integrity, auditability, and automated execution of contractual logic via smart contracts, thereby mitigating risks associated with single points of failure and data tampering in IIoT ecosystems [7,8].

The synergistic integration of QML and Blockchain within 6G-IIoT architectures is increasingly proposed as a holistic solution to these challenges [1,9,10]. QML could enhance the intelligence and efficiency of Blockchain operations by optimizing consensus mechanisms. At the same time, Blockchain could provide a verifiable, tamper-proof ledger for QML model updates and inferences, thereby fostering trust in distributed AI systems. Despite this promising convergence, the field remains fragmented and lacks a comprehensive analysis of its intellectual structure, evolution, and core research gaps. Existing reviews [11,12] are primarily descriptive or focus on a single technology; none have employed bibliometric methods to map the research landscape quantitatively or provided a critical meta-analysis of integrated QML-Blockchain frameworks. This study addresses this critical gap by conducting a rigorous bibliometric and meta-analysis of the convergence of QML and Blockchain for secure 6G-IIoT. Our contributions are as follows:

leftmirgin = * We present the first science-mapping study of this domain, analyzing 159 publications to visualize collaborative networks, thematic clusters, and temporal trends, providing an objective snapshot of the field's structure.
leftmiirgiin = * We move beyond description to a critical synthesis of QML and Blockchain capabilities, presenting quantitative performance metrics and identifying underexplored research avenues.
leftmiiirgiiin = * We propose a novel five-layer architectural framework that synthesizes bibliometric insights into a structured roadmap for future system design.
leftmivrgivn = * We provide a detailed analysis of limitations and a forward-looking perspective with specific, actionable recommendations for tackling key challenges such as quantum hardware maturity, consensus scalability, and empirical validation.

The remainder of this paper is organized as follows: Section 2 reviews the foundational concepts of adaptive IIoT, QML, and Blockchain. Section 3 details the Kitchenham-guided bibliometric methodology. Sections 4 and 4.2 present meta-analyses of QML and Blockchain, respectively. Section 4.3 explores their synergistic integration and presents the proposed framework. Section 5 discusses research gaps and future directions, and Section 6 provides a conclusive outlook.

2. Background study

This section establishes the foundational concepts, highlights the evolving demands of adaptive IIoT networks, and introduces the core principles of QML and Blockchain as enabling technologies.

2.1. Exploring evolving opportunities, trends, and demands in adaptive IIoT networks

Adaptive IIoT networks represent a significant advancement, enabling dynamic communication, intelligent decision-making, and seamless interaction between physical and digital components. These systems are critical in smart manufacturing, energy, healthcare, and logistics [13,14]. The IIoT ecosystem is expanding rapidly, with forecasts predicting over 41 billion connected devices by 2027 [15]. Central to adaptive IIoT is the processing of vast data streams for predictive maintenance and operational optimization [16].

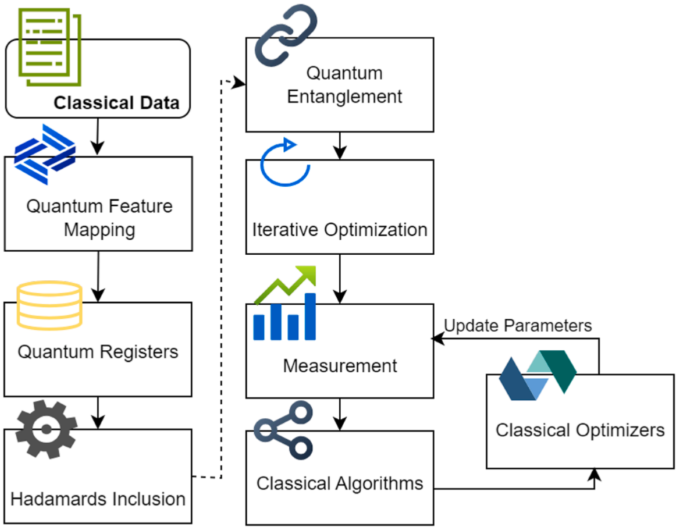

Figure 2. Quantum Machine Learning (QML) workflow.

This growth unlocks transformative opportunities. Real-time monitoring and predictive analytics help reduce downtime and improve safety [17,18]. Integration with 6G networks, edge computing, and AI-driven analytics further enhances adaptability by enabling decentralized decision-making and low-latency data processing [19,20]. As shown in Fig. 1, modular IIoT architectures comprising physical, network, middleware, and application layers have become standard for scalability [21].

Despite its potential, adaptive IIoT faces significant challenges. Massive data generation can create processing bottlenecks [22]. Interoperability remains a major hurdle due to the diversity of devices and protocols [16]. Cybersecurity is also critical; as IIoT networks expand, they are increasingly exposed to threats such as data breaches and DDoS attacks [16]. Emerging technologies such as QML and Blockchain are being explored to address these challenges [11,23].

2.2. Overview of Quantum Machine Learning

Quantum Machine Learning (QML) represents an interdisciplinary frontier that harnesses the principles of quantum mechanics to enhance classical machine learning algorithms. By leveraging quantum phenomena such as superposition and entanglement, QML can process information in fundamentally new ways, offering potential exponential speedups for specific problem classes, particularly those involving high-dimensional data and complex optimization [24,25].

In the context of IIoT, QML's potential is profound. IIoT systems generate massive, high-velocity data streams from myriad sensors. QML algorithms, such as Quantum Support Vector Machines (QSVMs) and Quantum Neural Networks (QNNs), can, in theory, analyze these datasets more efficiently than their classical counterparts. For instance, quantum parallelism enables the simultaneous evaluation of multiple states, which can drastically accelerate tasks such as feature selection, anomaly detection, and combinatorial optimization for resource scheduling [26,27]. A generalized QML workflow, illustrating the encoding of classical data into quantum states and subsequent quantum-influenced processing, is depicted in Fig. 2.

2.3. Key features of QML in IIoT

1. **Enhanced Data Processing Capabilities:** QML utilizes quantum parallelism, enabling the simultaneous processing of large datasets [28]. This capability is crucial in IIoT systems, where large volumes of sensor-generated data require real-time analysis. QML algorithms, such as QSVMs and QNNs, can efficiently handle high-dimensional datasets, outperforming classical methods in terms of speed and scalability [29].
2. **Scalability for Complex Networks:** As IIoT networks expand, computational demand increases significantly due to the number of interconnected devices and their interactions. QML provides a scalable solution by leveraging quantum entanglement and superposition to process data from multiple devices simultaneously, ensuring that large-scale IIoT networks maintain high efficiency without bottlenecks [26].
3. **Advanced Pattern Recognition and Anomaly Detection:** QML algorithms excel at recognizing complex patterns and anomalies in datasets due to their ability to represent and process nonlinear relationships more effectively than classical models [27].
4. **Improved Optimization for Resource Management:** Optimization is central to IIoT operations, including resource allocation, scheduling, and energy consumption. QML techniques, such as the Quantum Approximate Optimization Algorithm (QAOA), provide near-optimal solutions to combinatorial problems in real time, significantly enhancing operational efficiency in IIoT systems [26].

5. **Enhanced Security:** QML contributes to IIoT security by enabling advanced cryptographic techniques and improving intrusion detection systems. Quantum-enhanced algorithms, such as quantum Boltzmann machines, can effectively process vast amounts of network traffic to detect security breaches or anomalies [28]. Furthermore, QML supports quantum key distribution (QKD), which ensures secure communication between IIoT devices by using quantum principles to detect eavesdropping [30].
6. **Real-Time Decision Making:** QML algorithms enable faster decision-making by rapidly analyzing and synthesizing large datasets, an essential feature in time-critical IIoT applications such as autonomous vehicles, smart grids, and robotic systems. Quantum-enhanced reinforcement learning (QRL) can be particularly effective for adaptive control in dynamic industrial environments [31].

2.4. Quantum Machine Learning contribution and challenges

QML offers transformative contributions to adaptive IIoT systems by enhancing data processing capabilities, enabling real-time optimization, and improving anomaly detection. Its ability to process complex datasets in parallel allows IIoT systems to manage large-scale data more efficiently and make faster, more informed decisions, particularly in applications such as predictive maintenance and energy management [32,33]. However, practical QML deployment in IIoT faces several challenges:

1. **Hardware Limitations:** Current Noisy Intermediate-Scale Quantum (NISQ) processors suffer from limited qubit counts, short coherence times (typically <100 μs), and high error rates, restricting the complexity of executable algorithms [34].
2. **Algorithmic Maturity:** Many QML algorithms remain theoretical, with limited empirical evidence of their superiority over optimized classical algorithms for practical IIoT tasks [35].
3. **Integration Complexity:** Seamlessly integrating QML with existing classical IIoT edge-cloud infrastructures requires novel hybrid architectures and poses significant software engineering challenges [3].

2.5. Overview of Blockchain technology

Blockchain, fundamentally a distributed and immutable ledger, provides a decentralized framework for transactional integrity and trust among disparate parties without a central authority [36]. Its core innovation lies in cryptographically chaining blocks of data, making historical records practically tamper-proof. For IIoT, Blockchain's value proposition is multifaceted. It can secure device identity management, create an auditable trail for sensor data provenance, and automate multi-party industrial processes such as supply chain logistics, energy trading through self-executing smart contracts [7,23]. This mitigates risks associated with centralized data silos and single points of failure, which are critical vulnerabilities in large-scale industrial systems.

2.6. Key features of Blockchain in IIoT

1. **Decentralization:** Blockchain eliminates single points of failure by distributing control across multiple nodes in the network [8,37]. Unlike centralized systems that rely on a single authority, Blockchain enables IIoT devices to interact directly without intermediaries. This decentralization is critical in industrial environments where high availability and fault tolerance are essential for operations such as supply chain management and real-time monitoring [38].
2. **Transparency:** The immutable nature of Blockchain ensures transparency by allowing all participants to access a synchronized and tamper-proof record of transactions [39]. In IIoT systems, this transparency is vital for tracing device interactions and maintaining data integrity across processes such as quality control, compliance auditing, and stakeholder trust management [8,40].
3. **Security:** Security is a foundational feature of Blockchain integration with IIoT. Cryptographic techniques such as hashing and digital signatures safeguard data during transmission and storage [38]. In IIoT applications, where sensitive industrial data is frequently exchanged, Blockchain mitigates risks including data breaches, unauthorized access, and cyberattacks [41].
4. **Automation:** Smart contracts, self-executing agreements coded into the Blockchain, enable autonomous operations within IIoT networks [42]. These contracts automate tasks such as payment settlements, resource allocation, and device coordination, reducing human intervention and operational delays. For instance, smart contracts in energy management systems can autonomously regulate supply-demand dynamics based on real-time IIoT data [43,44].
5. **Scalability:** Blockchain supports scalability by allowing seamless integration of devices and transactions without degrading performance [45]. Advanced protocols such as sharding and layer-2 solutions enhance Blockchain's capacity to manage the vast number of interconnected devices typical in IIoT networks. This scalability is essential for applications, such as predictive maintenance, where large-scale sensor data must be processed and analyzed in near real-time [46].

2.7. Blockchain contribution and challenges

Blockchain technology offers critical contributions to adaptive IIoT systems by ensuring data integrity, fostering decentralization, and enabling automation through smart contracts. Its transparent, tamper-proof ledger guarantees the authenticity of data exchanged across IIoT devices, thereby enhancing decision-making and securing industrial transactions [40,47]. The decentralized architecture of Blockchain eliminates reliance on central authorities, instead using consensus mechanisms to validate data and protect IIoT networks from cyberattacks and single points of failure [48,49].

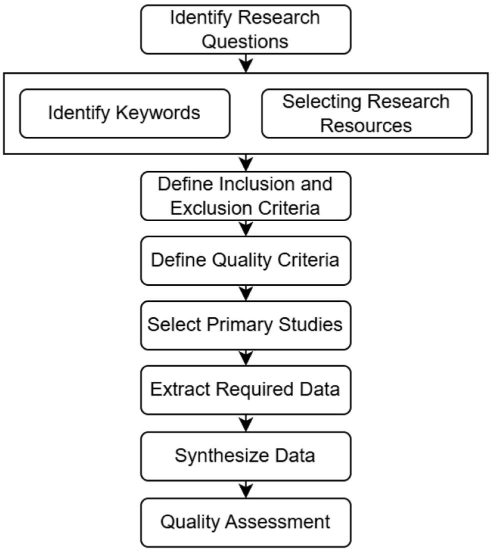

Figure 3. Execution process.

Smart contracts further extend Blockchain's utility by automating critical processes, such as triggering maintenance tasks when sensor data indicates potential failures. This reduces human intervention, improves response times, and enhances operational efficiency [50,51]. These features make Blockchain a powerful enabler of secure and autonomous IIoT ecosystems. Despite these advantages, Blockchain faces significant hurdles in IIoT environments:

1. **Scalability:** Traditional consensus mechanisms like Proof-of-Work (PoW) suffer from low transaction throughput and high latency, making them ill-suited for high-frequency IIoT data exchanges [45,52].
2. **Energy Consumption:** PoW-based Blockchains are notoriously energy-intensive, conflicting with the sustainability goals of many industries [52,53].
3. **Storage and Computational Overhead:** Maintaining a full copy of the ledger and performing cryptographic verifications can be prohibitive for resource-constrained IIoT devices [45,52,53].

2.8. Integrated QML-Blockchain in IIoT under 6G

The confluence of QML, Blockchain, and 6G is envisioned as a cornerstone for next-generation IIoT. The 6G infrastructure, with its sub-millisecond latency and ability to connect massive numbers of devices, provides the communication fabric needed to synchronize distributed QML inference and Blockchain consensus. In this integrated vision, QML acts as the "intelligent brain" for predictive security and optimization, while Blockchain serves as the "trusted spine" for integrity and decentralized coordination. For instance, a QML model at the edge could detect a subtle anomaly in motor vibration data, predicting an impending failure. This inference, once hashed and recorded on a lightweight Blockchain (using a PoA^2 consensus) [54], could automatically trigger a smart contract to order a replacement part and schedule maintenance, all within the latency bounds of a 6G network. This creates a closed-loop, self-healing industrial system. However, this integration remains largely conceptual. Foundational challenges include designing QML models that are robust to quantum noise, developing energy-efficient Blockchain consensus protocols capable of handling IIoT-scale transaction volumes, and creating standardized interfaces for seamless cross-layer orchestration. The following sections provide a systematic analysis of the research landscape to assess progress toward this vision.

3. Bibliometric method

Bibliometrics is a statistical methodology used to analyze books, journals, and scholarly articles, helping researchers evaluate scientific activity and research trends [55]. It provides a quantitative overview of developments within a specific domain and identifies influential publications, authors, and thematic clusters. In recent years, bibliometric analysis has gained traction in various disciplines, particularly in knowledge and data engineering [56]. Applications span knowledge management [57], data analysis and big data [58], data mining [59], data management [60], machine learning techniques [61], and text mining [62]. These studies offer insights into research productivity, citation dynamics, and emerging topics. To ensure a rigorous, transparent, and reproducible analysis, this study employed a systematic bibliometric review methodology guided by the Kitchenham et al. [63] execution protocol, as illustrated in Fig. 3.

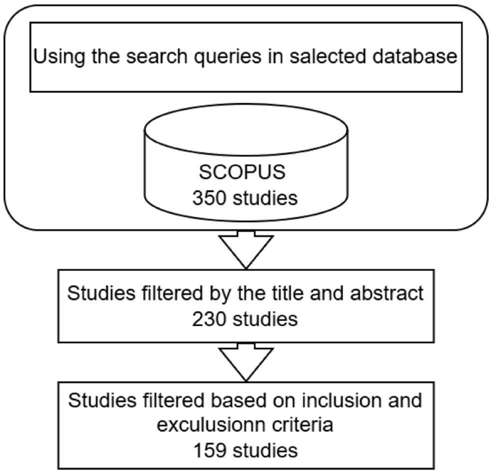

Figure 4. Primary study selection procedure.

3.1. Data source and search strategy

This study employed a structured bibliometric protocol to ensure analytical rigor and reproducibility. The Scopus database, managed by Elsevier, was selected due to its extensive multidisciplinary coverage of peer-reviewed literature, surpassing alternatives such as ScienceDirect and Web of Science in breadth and citation indexing [64,65]. A comprehensive search query was constructed to capture the core themes of QML, Blockchain, 6G, IIoT, and security: (TITLE-ABS-KEY (“Quantum Machine Learning" OR “QML" OR “Quantum Neural Network*" OR “Quantum AI") AND TITLE-ABS-KEY (“Blockchain" OR “Distributed Ledger" OR “Smart Contract*") AND TITLE-ABS-KEY (“6G" OR “Sixth Generation" OR “B5G") AND TITLE-ABS-KEY (“IIoT" OR “Industrial IoT" OR “Industrial Internet of Things" OR “Industry4.0″). The search was constructed to capture publications from January 2022 onward, reflecting the field inception. The final query was executed on December 22, 2024, thereby including all relevant publications indexed in Scopus up to that date.

3.2. Inclusion and exclusion criteria

A systematic screening process was applied using predefined criteria:

- **Inclusion:** Peer-reviewed journal articles, conference proceedings, and review articles published in English that explicitly addressed the integration or concurrent application of QML and Blockchain technologies within the context of 6G and IIoT security.
- **Exclusion:** Non-peer-reviewed publications, editorials, letters, non-English papers, and studies that mentioned the keywords only peripherally without a substantive technical contribution to the integration theme. Duplicate publications were also removed.

3.3. Data extraction and analysis

The automatic search on the Scopus database returned 350 studies in the initial search. After the first iteration, during which titles and abstracts were screened, unrelated studies were excluded, leaving 230 relevant studies. In the second iteration, 71 studies were removed after applying the inclusion and exclusion criteria, resulting in a final set of 159 Scopus documents used for the analysis, as shown in Fig. 4.

Metadata including publication year, authors, affiliations, source titles, keywords, and citation data were extracted from Scopus in `.csv` format. Bibliometric analysis was conducted using VOSviewer (version 1.6.18), a robust tool for constructing and visualizing bibliometric networks [66,67]. We employed three primary types of analysis:

1. **Co-authorship Analysis:** To map collaboration networks between countries and institutions.
2. **Co-occurrence Analysis:** To identify thematic clusters based on author keywords.
3. **Citation Analysis:** To identify influential sources and documents.

The analysis combined quantitative metrics (publication/citation counts) with qualitative interpretation of network visualizations to derive meaningful insights into the research landscape. Fig. 5 illustrates the methodological flowchart, starting from topic definition and keyword selection in Scopus to CSV export and analysis in VOSviewer. The diagram outlines each stage of data curation and visualization, ensuring transparency and reproducibility.

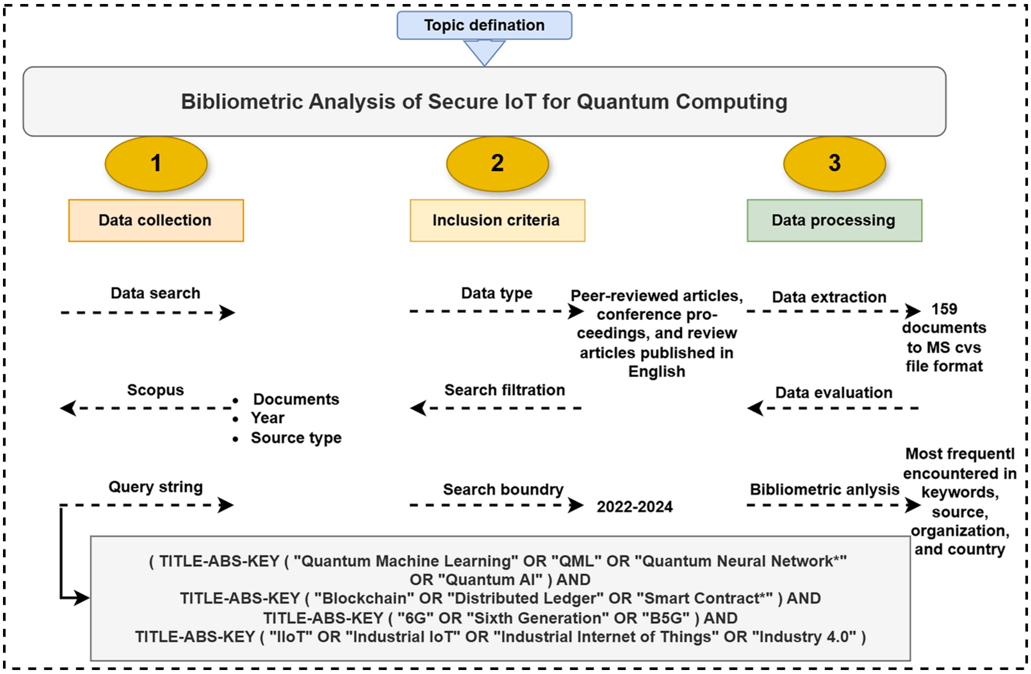

Figure 5. Flowchart illustrating the systematic data collection process from topic definition and database search (Scopus) to data extraction and evaluation, prepared for bibliometric analysis.

Table 1
Annual publication output.

Year	Frequency	Percentage % (N = 159)
2022	48	30.2%
2023	63	39.6%
2024	48	30.2%

Table 2
Distribution of document and source types.

Category	Type	Frequency	% (N = 159)
Document Type	Article	71	44.7%
	Conference Paper	22	13.8%
	Review	33	20.8%
	Book Chapter	24	15.1%
	Other	9	5.6%
Source Type	Journals	109	68.6%
	Books/Proceedings	50	31.4%

3.4. Bibliometric results and discussion

3.4.1. Publication trends and document types

The annual publication output, presented in Table 1, reveals the field's dynamic growth. A significant acceleration occurred from 2022 onward, with a 75% increase from 2022 to 2023. This trend underscores the rising recognition of the topic's importance alongside advancements in 6G standardization and quantum computing. The distribution of document types (Table 2) shows that journal articles constitute the majority (44.7%), indicating a maturing research discourse. The substantial proportion of review papers (20.8%) further suggests a community effort to synthesize knowledge in this rapidly evolving area.

3.4.2. Keyword analysis and thematic clusters

Keyword co-occurrence analysis provides profound insights into the intellectual structure of emerging 6G research. Of the identified keywords, 21 met the minimum threshold of 5 occurrences. The network visualization (Fig. 6) and frequency data (Table 3) reveal four distinct, yet interconnected, thematic clusters:

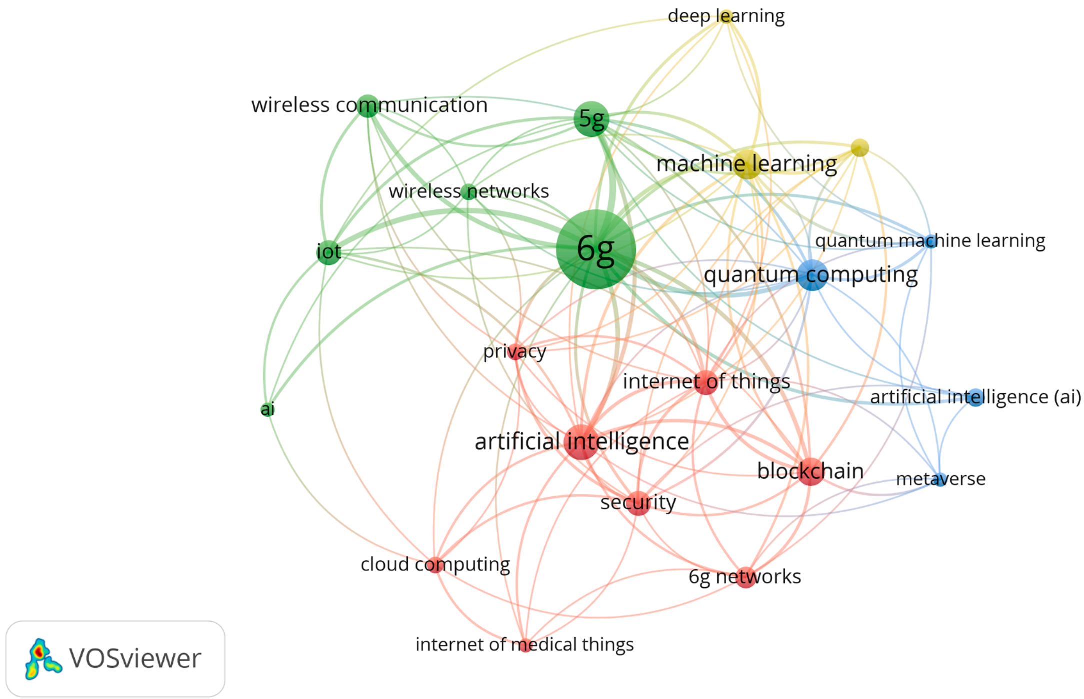

Figure 6. Network visualization of author keyword co-occurrence. Minimum number of occurrences: 5. Four distinct thematic clusters are identified.

1. **Cluster 1 (Green): 5G and 6G Wireless Connectivity** centered around '6G,' '5G,' 'Wireless Communication,' and 'IoT,' this cluster represents the foundational technologies driving the evolution from 5G to 6G networks, emphasizing advancements in wireless systems and connectivity architectures.
2. **Cluster 2 (Red): AI-Driven Security and Privacy** dominated by 'Artificial Intelligence,' 'Security,' 'Blockchain,' 'Privacy,' and 'Cloud Computing,' this cluster focuses on the critical role of AI in enhancing the resilience, trust, and data protection of next-generation communication infrastructures.
3. **Cluster 3 (Yellow): Machine Learning and Data Intelligence** featuring 'Machine Learning,' 'Deep Learning,' and related keywords, this cluster reflects the growing influence of intelligent data-driven techniques in optimizing network performance, automation, and decision-making within the 6G ecosystem.
4. **Cluster 4 (Blue): Quantum Technologies and Future Computing** comprising 'Quantum Computing,' 'Quantum Machine Learning,' and 'Metaverse,' this cluster illustrates the integration of quantum paradigms with AI and communication networks, signifying a frontier for computational and communication convergence.

The strong interconnections between Clusters 1, 2, and 4, particularly through '6G,' 'AI,' and 'Quantum Computing,' highlight the interdisciplinary nature of next-generation network research, where intelligent, secure, and quantum-enhanced communication systems form the backbone of future digital infrastructures.

The network visualization map of the author's keywords is presented in Fig. 6, highlighting the most frequently occurring terms across the analyzed publications. This visualization reflects thematic concentrations and emerging research trends within the domain. A conceptual bibliometric map was generated using VOSviewer to illustrate the relationships and co-occurrence patterns among keywords [68]. This technique enables the identification of semantic clusters and structural linkages, offering insights into how research topics are interconnected.

3.4.3. Geographic and institutional distribution

The geographic distribution of research output (Table 4, Fig. 7) highlights a globally distributed effort led by India (37.7%), followed closely by the United States and South Korea (12.6% each). Saudi Arabia and China also show significant contributions. This indicates worldwide recognition of the topic's strategic importance. The collaboration network map shows strong intra-country collaborations but sparser international links, suggesting an area for future growth. At the institutional level (Table 5), contributions are distributed, with no single institution dominating. Taif University (Saudi Arabia) stands out with the highest citation count per publication among the listed institutions, indicating high-impact research despite a modest output volume.

3.4.4. Source analysis

Fig. 8 illustrates the most active and influential journals contributing to research on "Quantum Machine Learning" (QML), "6G networks," and "Security," based on a dataset of 159 publications. Among these, IEEE Access leads with 11 documents, reflecting

Table 3
Popular keywords.

Author Keywords	Frequency	Percentage (N = 159) (%)
6G	56	35.22%
5G	18	11.32%
Artificial Intelligence	18	11.32%
Machine Learning	14	8.81%
Internet of Things	11	6.92%
Blockchain	13	8.18%
IoT	11	6.92%
Quantum Computing	15	9.43%
Security	11	6.92%
Quantum Communication	7	4.40%
Wireless Communication	10	6.29%
Privacy	6	3.77%
Quantum Machine Learning	5	3.14%
6G Network	9	5.66%
Cloud Computing	6	3.77%
Deep Learning	5	3.14%
Wireless Network	6	3.77%
Artificial Intelligence (AI)	7	4.40%
Internet of Medical Things	5	3.14%
Metaverse	5	3.14%
AI	5	3.14%

Table 4
Top contributing countries/regions.

Country/Region	Frequency	Percentage (N = 159)	Citations
India	60	37.74%	730
United States	20	12.58%	148
South Korea	20	12.58%	393
Saudi Arabia	16	10.06%	400
China	15	9.43%	384
United Kingdom	12	7.55%	98
Canada	11	6.92%	227
Malaysia	10	6.29%	413
Finland	10	6.29%	150
Pakistan	8	5.03%	156
United Arab Emirates	7	4.40%	56
Bangladesh	6	3.77%	136
Germany	6	3.77%	52
Spain	6	3.77%	65
Lebanon	6	3.77%	154
Ireland	6	3.77%	98
Turkey	5	3.14%	211
Sweden	5	3.14%	55
Iraq	5	3.14%	18

Table 5
Most influential institutions with a maximum of 2 publications.

Institution	Frequency	Citations
Chitkara University, Punjab, India	2	16
Zhejiang University, Hangzhou, China	2	38
Taif University, Saudi Arabia	2	89
Queen's University Belfast, UK	2	32
Sunyani Technical University, Ghana	2	32
University of Oulu, Finland	2	17

its prominence in publishing interdisciplinary and emerging technology research. Other notable sources include Sensors, Alexandria Engineering Journal, IET Quantum Communication, Computer Networks, Electronics (Switzerland), IEEE Communications Surveys & Tutorials, Sustainability (Switzerland), ICT Express, IEEE Open Journal of the Communications Society, and IEEE Internet of Things Journal. Additional contributions were observed from journals such as Security and Privacy Schemes for Defence, Signals and Communication Technology, Challenging and Risk Involved, International Journal of Communications, Journal of King Saud University, Journal of Network and Computer Applications, and Physical Communication. These journals collectively represent the core publication venues for research at the intersection of QML, Blockchain, and IIoT security in the context of 6G networks. Their

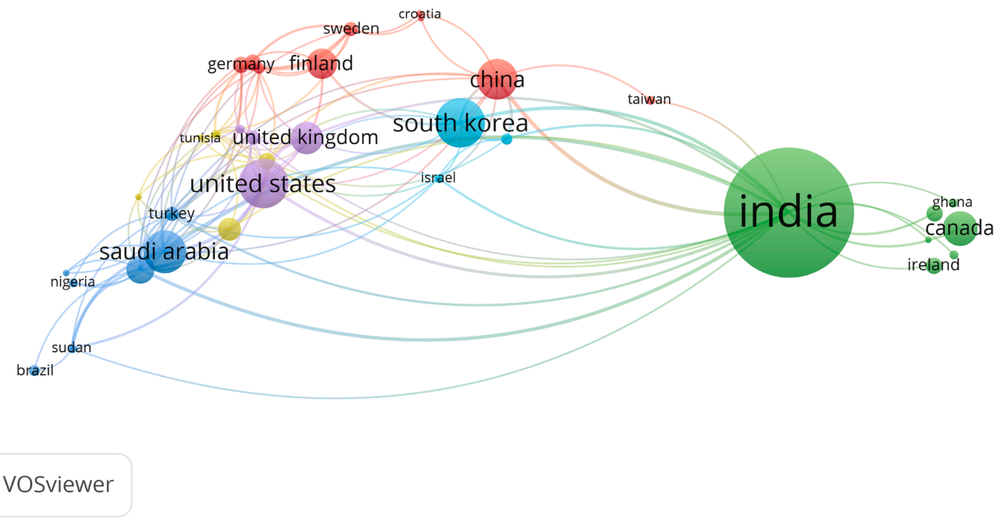

Figure 7. Network visualization of international co-authorship. Minimum number of documents per country: 2.

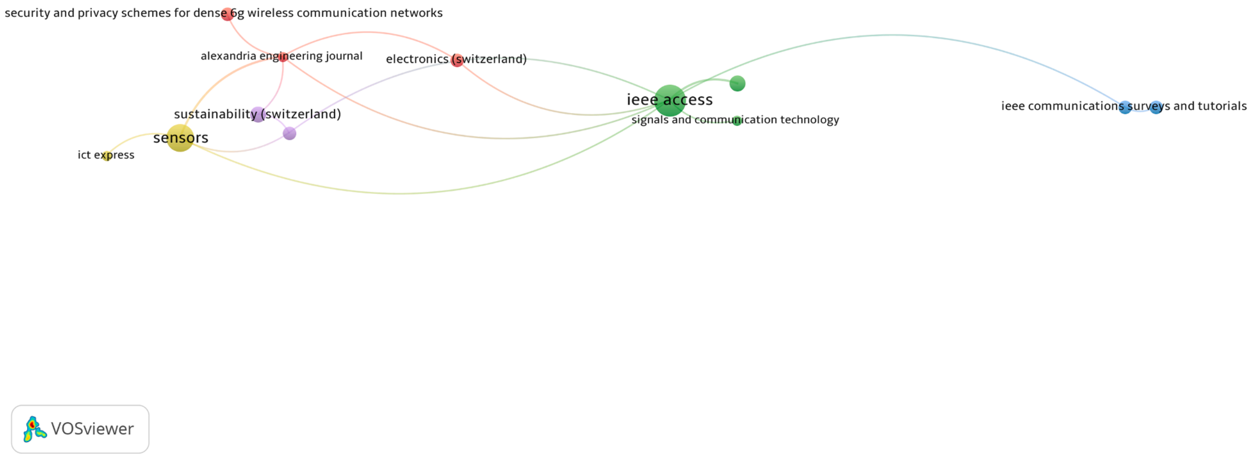

Figure 8. Network visualization map of co-occurrences of sources. Types of analysis = Source, Counting method: Full counting, Minimum number of occurrences = 2. This publication pattern indicates that contributions are bridging the gaps between computer science, electrical engineering, and societal impact, ensuring rapid dissemination across relevant engineering communities.

inclusion underscores the field's interdisciplinary nature and the growing interest across engineering, computing, and sustainability. Table 6 provides a detailed breakdown of these source titles and their respective document contributions (Fig. 9).

4. Meta-analysis of emerging technologies

4.1. Meta-analysis of QML in real-world IIoT systems

This section transitions from bibliometric mapping to a critical meta-analysis of QML's proposed applications in IIoT, evaluating its reported performance and identifying gaps between promise and practice.

4.1.1. QML applications in IIoT, edge, and next-generation networks

QML enhances IIoT, edge, and next-generation network performance by addressing classical scalability and latency limits. For instance, Yun et al. [69] achieved 8% higher task accuracy and 14.2 ms lower latency using QMARL in smart factories, while Peelam et al. [70] improved IoT network throughput through quantum optimization. Other advances include Melnikov et al. [71] noise-mitigation for NISQ systems and Hua et al. [72] six-qubit protocol for secure IoT communication. Satpathy et al. [73] used variational QML models for power data, achieving 98.10% accuracy with minimal storage, and Gill [74] proposed a Quantum-Blockchain Edge framework for secure and scalable processing. In 6G, Narottama et al. [75] demonstrated that QSVMs and quantum reinforcement learning outperform classical models in MIMO and UAV optimization, while Cao et al. [76] achieved efficient resource allocation via DT-Slice-Soft-6G.

Table 6
Most active source titles with at least 2 publications.

Source Title	No. of Documents	% (N = 159)	Citations	% (N = 1352)
IEEE Access	11	6.91%	242	17.89%
Sensors	9	5.66%	239	17.67%
Alexandria Engineering Journal	2	1.25%	129	9.54%
IET Quantum Communication	3	1.88%	33	2.44%
Computer Networks	4	2.51%	66	4.79%
Electronics (Switzerland)	3	1.88%	58	4.28%
IEEE Communications Surveys and Tutorials	3	1.88%	197	14.57%
Sustainability (Switzerland)	4	2.51%	54	3.99%
ICT Express	2	1.25%	75	5.54%
IEEE Open Journal of the Communications Society	3	1.88%	41	3.03%
Security and Privacy Schemes for Defence	3	1.88%	1	0.07%
Signals and Communication Technology	2	1.25%	1	0.07%
Challenging and Risk Involved	4	2.52%	7	0.52%
IEEE Internet of Things Journal	2	1.25%	103	7.62%
International Journal of Communications	3	1.88%	19	1.41%
Journal of King Saud University - Computer and Information Sciences	2	1.25%	64	4.73%
Journal of Network and Computer Applications	2	1.25%	1	0.07%
Physical Communication	2	1.26%	22	1.63%

Figure 9. Network visualization map of the co-authorship. Unit of analysis = Organizations, Counting method: Full counting, Minimum number of documents of an organization = 2.

4.1.2. Security vulnerabilities and countermeasures in QML systems

Despite these gains, QML introduces new vulnerabilities. Kundu and Ghosh [77] and Nguyen et al. [78] identified risks such as adversarial perturbations, model poisoning, and compilation attacks that can manipulate or leak model data. Defense strategies include Quantum Adversarial Training, QuGANs, defensive distillation, and hardware-based safeguards like QuPUFs, Split Compilation, and Dummy Gate Insertion. Collectively, these studies show that while QML offers strong potential for IIoT and 6G security, real-world resilience depends on protection at algorithmic, architectural, and hardware levels. Tables 7 and 8 summarize these studies and performance claims, which are largely simulation-based rather than field-tested.

A critical analysis of the application focus (Table 9) reveals a strong emphasis on encryption and anomaly detection, which aligns with immediate security concerns. However, areas with significant long-term industrial impact, such as predictive maintenance and resource allocation, are comparatively underexplored, representing a key research gap.

Table 7
Summary of representative QML studies in IIoT and related domains.

Ref.	Contribution	Techniques	Application Domain
[69]	Proposed Quantum Multi-Agent Reinforcement Learning (QMARL) for distributed robot coordination, improving accuracy and latency.	Quantum reinforcement learning using Centralized Training and Decentralized Execution (CTDE).	Smart factory automation and IIoT robotics.
[70]	Surveyed quantum computing applications and algorithms for IoT security and network optimization.	Review of quantum algorithms and simulation techniques.	IoT security and network optimization (Review).
[71]	Reviewed quantum machine learning fundamentals, from physics to software engineering implementation.	Tutorial on QML concepts, algorithms, and error mitigation techniques.	Quantum-enhanced AI (Tutorial/Review).
[72]	Introduced a hierarchical quantum communication protocol using six-qubit entanglement for enhanced privacy.	Hybrid quantum communication protocol with entangled-state encryption.	Secure IoT communication and data protection.
[73]	Applied QML algorithms for classification of IoT-based power generation data in extreme environments.	$UU^\dagger$, variational $UU^\dagger$, and Quantum Neural Network (QNN) models.	Energy-efficient IoT sensing and data classification.
[74]	Presented a vision for integrating quantum computing and blockchain in serverless edge architectures for IoT.	Conceptual framework for quantum-blockchain-edge integration.	Serverless edge computing for IoT (Vision paper).
[75]	Surveyed quantum machine learning techniques and their potential applications in 6G wireless communications.	Review of QML algorithms including QSVMs and quantum reinforcement learning.	6G wireless communications (Survey).
[76]	Proposed DT-Slice-Soft-6G framework for resource allocation using quantum-assisted Digital Twins.	Heu-DT-Slice-6G algorithm based on Markov random modeling.	Quantum-enabled 6G resource management and network slicing.

Table 8
Reported quantitative performance metrics from QML studies.

Ref.	Application Domain	QML Model	Accuracy (%)	Latency (ms)
[69]	Multi-Robot Control	QMARL (CTDE)	96.5	14.2
[70]	IoT Security	Quantum Computing Applications	N/A	N/A
[72]	Secure IoT Communication	Six-Qubit Entangled Protocol	N/R†	N/R†
[71]	Quantum AI Modeling	Quantum ML Review	N/A	N/A
[73]	Power Data Classification (IoT)	Variational $UU^\dagger$	98.1	11.3
[74]	Edge-Blockchain Integration	Quantum-Blockchain Vision Model	N/A	N/A
[75]	6G Network Optimization	Survey of QML for 6G	N/A	N/A
[76]	Digital Twin-Based 6G Allocation	Heu-DT-Slice-6G (QML-Assisted)	96.7	12.9

4.2. Meta-analysis of Blockchain in real-world IIoT systems

This section moves from bibliometric mapping to a focused meta-analysis of Blockchain use in IIoT, analyzing its architecture, progress in consensus, and adaptability for Industry 5.0. It assesses Blockchain's role in improving trust, scalability, and interoperability while identifying gaps between proposed frameworks and actual deployment.

Table 9
Critical analysis of QML application focus in IIoT security.

Ref.	Anomaly Detection	Quantum Encryption	Error Mitigation	Predictive Maintenance	Resource Allocation
[79]	✓	✓	✗	✗	✗
[69]	✗	✗	✓	✗	✗
[71]	✗	✗	✓	✓	✗
[70]	✓	✓	✗	✓	✓
[72]	✗	✓	✗	✗	✗
[73]	✓	✗	✗	✓	✗
[74]	✗	✓	✗	✗	✓
[75]	✗	✗	✗	✗	✓
[76]	✗	✗	✗	✗	✓
[77]	✓	✓	✓	✗	✗

4.2.1. Evolution of consensus mechanisms

A dominant theme in recent literature is the shift away from energy-intensive Proof-of-Work (PoW) toward lightweight, deterministic, and energy-efficient consensus models suitable for IIoT. Saleh et al. [80] introduced Directed Acyclic Graph (DAG) structures for high-throughput IIoT, enabling parallel validation and asynchronous transaction confirmation. Xu et al. [81] analyzed variants of Proof-of-Stake (PoS) for improved energy performance and scalability. Kim et al. [54] proposed the Proof-of-Authority-and-Association (PoA^2) consensus, achieving deterministic finality and low-latency operation, optimized explicitly for IIoT environments.

4.2.2. Security and trust management in IIoT

Blockchain has been widely applied to strengthen trust management and authentication in industrial networks. Its decentralized and immutable characteristics address IIoT challenges such as reliance on centralized authority, data silos, and trust breaches [82,83]. Lahbib et al. [82] classified Blockchain-based trust management (TM) in IIoT into four categories, emphasizing secure evidence collection, autonomy, and confidentiality of trust interactions. Ghovanlooy Ghajar et al. [84] designed Schloss, a distributed Blockchain framework in which industrial nodes construct private Blockchains to share operational data securely. Asaithambi et al. [85] implemented Blockchain-based smart contracts and reputation systems for end-to-end authentication in industrial networks. Gong et al. [86] developed BCoT Sentry, an identity-authentication framework that combines traffic-feature learning and smart contracts to validate device identities in IIoT.

4.2.3. Scalability and edge integration

Scalability and computational overhead remain critical limitations in the Blockchain-IIoT convergence, especially under real-time industrial constraints [83,87]. Several works have addressed these issues through architectural and consensus-level optimizations. In the study by Asaithambi et al. [85] proposed Proof of Authentication (PoAh), a resource-efficient consensus integrated with edge computing. It reduces authentication time and improves throughput in constrained environments. Wu and Ansari [88] introduced DPA-PBFT, a Dynamic Practical Byzantine Fault Tolerance algorithm that minimizes communication overhead and enhances synchronization among non-peer nodes, suitable for time-critical IIoT applications. Hybrid frameworks combining cloud computing and Blockchain have been developed, where IoT devices maintain lightweight hash chains while block data is stored in the cloud to reduce on-device computation and storage costs [83].

4.2.4. Supply chain and traceability applications

Blockchain also contributes to industrial transparency and accountability through traceable data management. Al-Rakhami and Al-Mashari [89] developed a lightweight Blockchain-IoT trust model enabling real-time data verification among supply chain actors, reducing latency and eliminating intermediaries. Vern et al. [90] presented a Blockchain-enabled traceability framework for agri-food supply chains, validated through a proof-of-concept deployment in honey and coriander powder logistics. Their study showed that Blockchain improves product transparency and stakeholder trust while outlining the operational and cost considerations required for practical adoption.

4.2.5. Synthesis of observations

The reviewed studies reveal that successful Blockchain integration in IIoT depends on selecting platforms and consensus mechanisms tailored to industrial constraints. Frameworks such as PureChain and PoA^2 enable trusted authority validation with association mapping [54]. PureChain delivers a 230% increase in throughput and a 70% reduction in latency compared to Ethereum and Hyperledger [91], while platforms like Hyperledger Fabric and IOTA Tangle provide modular consensus and DAG-based scalability for low-energy, decentralized coordination [92]. This trend underlines the growing preference for hybrid, low-latency, and interoperable Blockchain systems optimized for IIoT operations. Table 10 summarizes key Blockchain studies. A critical synthesis reveals that while theoretical frameworks are abundant, empirical validation in large-scale, realistic IIoT testbeds is rare. Most performance metrics are based on simulations or small private networks.

Table 11 provides a comparative analysis of consensus mechanisms, clearly demonstrating the trade-offs in performance. PoA^2 and DAG emerge as the most suitable for IIoT due to their low latency and high throughput. However, their security models under byzantine conditions in vast IIoT networks require further investigation.

Table 12 presents a critical analysis of Blockchain applications in IIoT.

Table 10
Summary of representative Blockchain studies in IIoT.

Ref.	Contribution	Techniques / Models	Application Domain
[7]	Blockchain-enabled secure frameworks for IIoT in 6G.	Permissioned ledgers, smart contracts, edge validation.	IIoT security and authentication.
[80]	DAG-based ledger structures for high-throughput IIoT.	Directed Acyclic Graph (DAG) consensus.	Lightweight edge ledger for mMTC.
[81]	Analysis of PoS for low-energy IIoT.	Proof-of-Stake (PoS) variants.	Energy-constrained IIoT networks.
[54]	PureChain: Proof-of-Authority-and-Association (PoA^2).	PoA^2 consensus, transaction-level finality.	Low-latency industrial transaction validation.
[82]	Trust management architecture for device-level IIoT systems.	Blockchain-based trust interaction and data management.	Industrial device trust and verification.
[85]	Lightweight Blockchain-assisted edge computing model.	Proof-of-Authentication (PoAh) consensus.	Scalable edge authentication for IIoT.
[88]	Dynamic PBFT for high-throughput industrial systems.	DPA-PBFT consensus mechanism.	Real-time synchronization in IIoT.
[89]	Blockchain-integrated supply chain model for IIoT.	Lightweight trust model with decentralized ledger.	Supply chain traceability and validation.
[90]	Blockchain-based traceability framework for agri-food supply chains.	Permissioned Blockchain with proof-of-concept deployment.	Agri-food traceability and supply chain transparency.

Table 11
Comparative consensus metrics across major Blockchain frameworks for IIoT systems.

Consensus Type	Throughput (TPS)	Finality Time (ms)	Energy per Tx (J)	Scalability (IIoT Nodes)
PoW	7–15[93]	3600–7200 [94]	700 [95]	Low (centralized mining)
PoS [81]	1000–4000 [96]	100–500 [97]	0.05 [98]	Moderate (delegated validation)
DAG [80]	500–1000 [99]	10–100 [100]	0.02 [101]	High (parallel validation)
PoA^2 [91]	230% improvement	70% reduction	N/R	Very High (trusted authorities with association mapping)

Table 12
Critical analysis of Blockchain application focus in IIoT.

Ref	Decentralization	Consensus Efficiency	Smart Contracts/Automation	Energy Efficiency	Edge Orchestration/Testbed
[7]	✓	✗	✓	✗	✓
[80]	✓	✓	✗	✓	✗
[81]	✓	✓	✗	✓	✗
[9]	✓	✗	✓	✗	✓
[10]	✓	✗	✓	✗	✗
[54]	✓	✓	✗	✓	✓

4.3. Meta-analysis of QML-Blockchain convergence and proposed framework

4.3.1. Case study

Recent case studies show strong progress in quantum-enhanced and Blockchain-secured IIoT systems, including Zhang et al. [102] on quantum-inspired resource scheduling for 6G, and Chen et al. [103] on Blockchain-secured digital twins for industrial monitoring. Patel et al. [104] smart-grid platform that combines quantum ML, smart contracts, and secure energy prediction. Further advancements include Kim et al. [105] federated and quantum ML framework for factory-scale analytics, Okafor et al. [106] PureQuantum QKD-enhanced Blockchain for validator security, and Lee et al. [107] field-tested system for Blockchain-based spectrum allocation and trusted QML anomaly detection in manufacturing environments (Table 13).

4.3.2. Synergistic integration and proposed framework

The bibliometric analysis confirmed the conceptual synergy between QML and Blockchain, but the meta-analysis reveals that their practical integration remains in its infancy. Most studies discuss the potential in isolation. Actual convergence research, where the output of one technology directly influences or optimizes the operation of the other, is scarce. The primary challenge is cross-layer orchestration. The latency between a QML inference and its subsequent validation and recording on a Blockchain must be within the operational deadlines of the IIoT application (e.g., for real-time control). This requires co-designing QML algorithms and Blockchain

Table 13
Comparison of algorithms, system prototypes, validation methods, and datasets.

Ref	Algorithms	Prototype / System	Validation Results	Datasets
[102]	Quantum Variational Models, Blockchain Consensus	6G Network Simulator	Latency, Resource Utilization, Security Metrics	Synthetic IIoT Traffic
[103]	Machine Learning, Blockchain Audit Trails	Industrial Digital Twin Framework	Fault Detection Accuracy, Event Traceability	Manufacturing Sensor Data
[104]	Quantum SVM, Smart Contract Automation	Energy IoT Smart Grid Prototype	Classification Accuracy, Secure Transaction Validation	Smart Meter Data Streams
[105]	Federated QML Models, Blockchain Privacy Layer	Industrial Edge Computing Network	Privacy Preservation, Scalability, Consensus Agreement Rate	Factory Sensor Benchmarks
[106]	BB84 QKD, PoA Consensus	Quantum-Secured Blockchain	Quantum key accuracy, Eavesdropping detection	Smart grids, Industrial IoT
[107]	ML-Based Anomaly Detection, Blockchain Identity Management	IIoT Experimental Testbeds	Security Performance, End-to-End Throughput	IIoT Deployment Data

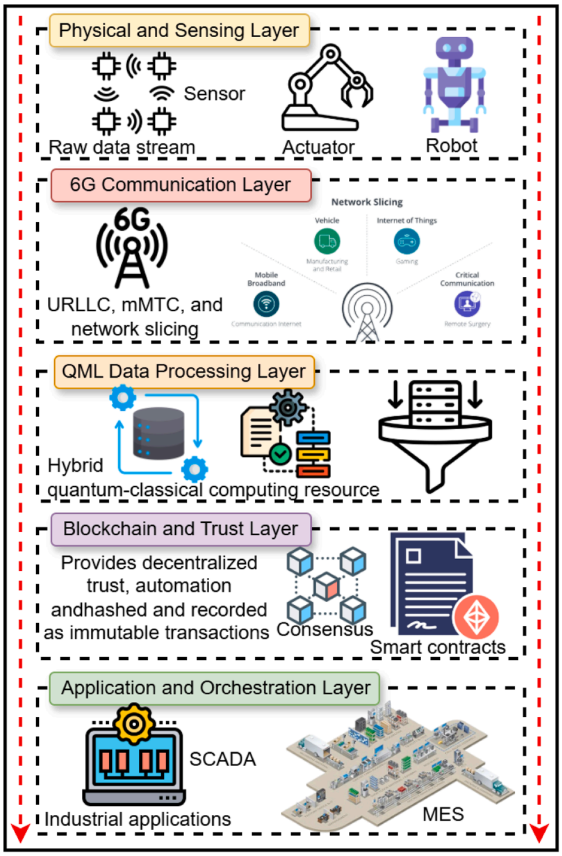

Figure 10. Proposed five-layer QML-Blockchain integration framework for secure and adaptive 6G-IIoT networks.

consensus protocols. To address this gap and provide a structured roadmap, we propose a novel five-layer integration framework, depicted in Fig. 10. This layered structure offers a concise blueprint for future work on QML-Blockchain convergence in 6G-enabled IIoT environments.

The integrated architecture for 6G-IIoT can be described as a tightly coupled pipeline that links sensing, communication, intelligence, and decentralized trust. The physical layer consists of IIoT devices that generate continuous data streams from industrial processes. These data flows traverse a 6G communication layer that provides ultra-reliable, low-latency links, massive device support, and network slicing for deterministic performance. The processed data reaches a quantum-enhanced analytics layer where hybrid QML models execute real-time inference for tasks such as anomaly detection, feature extraction, and system optimization. The resulting decisions are then secured in a Blockchain-based trust layer, where lightweight mechanisms such as PoA[2] or DAG consensus

Table 14
Comparative analysis of this study against existing reviews.

Study	Bibliometric Analysis	Meta-Analysis	QML-Blockchain Focus	Integration Framework	6G-IIoT Context
[11]	✗	✗	✓	✗	✓
[12]	✗	✗	✓	✗	✓
[10]	✗	✗	✓	✗	✓
[9]	✗	✗	✓	(Conceptual)	✓
This Study	✓	✓	✓	**✓(5-Layer)**	✓

Table 15
Synthesis of research gaps and future directions.

Research Gap	Description	Suggested Way Forward	Future Recommendation
Empirical Validation	Lack of real-world testbeds; most results are simulation-based.	Develop hybrid hardware-in-the-loop testbeds integrating QPUs (e.g., via cloud access) with Blockchain platforms (PureChain, Hyperledger Besu, Ethereum).	Establish open-access, standardized IIoT testbeds for benchmarking latency, throughput, and energy consumption.
Quantum Hardware Maturity	NISQ device limitations (coherence time, error rates) restrict model complexity.	Focus on hybrid quantum-classical algorithms (VQAs) and design QML models specifically for noise resilience.	Foster industry-academia collaborations with quantum hardware vendors to test algorithms on real devices using industrial datasets.
Consensus Scalability	Performance of PoA^2, DAG under massive IIoT node density (>>10,000 devices) is unproven.	Develop and simulate novel sharding techniques and cross-chain protocols tailored for IIoT network partitions.	Implement large-scale network simulations and testbed experiments to validate consensus performance at scale.
Cross-Layer Orchestration	Lack of standards and protocols for synchronizing QML inference with Blockchain finality.	Design a dedicated “Orchestrator" module (as in our framework) with APIs for workload scheduling and resource management.	Propose standardizing interfaces (APIs) between QML middleware and Blockchain layers through bodies such as IEEE and IETF.
Energy Efficiency	The combined energy footprint of QML and Blockchain operations at the edge is unknown.	Co-design energy-aware QML algorithms and ultra-low-power consensus mechanisms. Develop accurate energy models.	Conduct life-cycle assessment (LCA) studies to evaluate the total energy cost and sustainability of integrated systems.
Security & Privacy	Vulnerability to quantum attacks (Shor’s algorithm) on classical Blockchain cryptography.	Integrate post-quantum cryptography (PQC) standards (e.g., CRYSTALS-Kyber, Dilithium) into Blockchain frameworks.	Mandate the migration to PQC for all new Blockchain-IIoT projects to ensure long-term security.

ensure fast, verifiable, and tamper-proof recording of system events while smart contracts automate operational logic. At the top, an application and orchestration layer integrates SCADA, MES, and other industrial platforms, coordinating model updates, enforcing policies, and managing Blockchain resources across the entire stack.

4.3.3. Comparative analysis with existing reviews

To explicitly establish the novelty of this work, Table 14 provides a comparative analysis against prior relevant survey and review articles. This highlights our unique contribution in providing a quantitative, bibliometric foundation and a structured integration framework.

5. Research gaps and future directions

The preceding analysis reveals a field rich in potential but facing significant hurdles to practical realization. Table 15 synthesizes the critical research gaps and proposes concrete future directions.

5.1. Limitations of the present study

This study has several limitations. The bibliometric analysis relied solely on Scopus. While comprehensive, it may have missed relevant works indexed in other databases, such as Web of Science or IEEE Xplore. The focus on English-language publications may introduce a language bias. Furthermore, as a review article, its conclusions are derived from the analysis of existing literature rather than primary experimental validation. Future work should involve empirical testing of the proposed framework and expanding the bibliometric data source.

6. Future prospects and outlook

The convergence of QML and Blockchain for 6G-IIoT security is poised at a critical juncture, transitioning from theoretical proposition to a domain demanding rigorous engineering and validation. The bibliometric evidence points to rapidly growing interest, but the meta-analysis underscores a significant maturity gap. The future research agenda must be aggressively oriented toward empirical validation. The proposed five-layer framework serves as a blueprint, but its layers must be instantiated and tested in hardware-in-the-loop environments that mimic real-world IIoT constraints. This requires a paradigm shift from isolated technology development to integrated system co-design. Key priorities include:

- **Hardware-Software Co-design:** Developing QML algorithms that are not only accurate but also “NISQ-aware," and pairing them with Blockchain consensus protocols that are “IIoT-scale-aware."
- **Standardization and Benchmarking:** The community must urgently define standardized performance metrics (e.g., end-to-end inference-to-action latency) and create open benchmark datasets to enable fair comparison and accelerate progress.
- **Quantum Resilience:** The integration of post-quantum cryptography is not a future consideration but a present-day necessity for any Blockchain system intended for long-term deployment in critical infrastructure.
- **Explainability and Trust:** As QML models make increasingly autonomous decisions, techniques for Explainable Quantum AI (XQAI) will be vital to ensure transparency, accountability, and regulatory compliance in industrial settings.

In conclusion, while the path forward is challenging, the potential payoff is a fundamental transformation of industrial systems into secure, intelligent, and truly autonomous ecosystems. This study has provided a comprehensive map of the current landscape and a compass for the journey ahead. The next phase of work must be characterized by collaboration, standardization, and a relentless focus on practical implementation.

Conflict of interest

The authors declare that there is no conflict of interest in this paper.

CRediT authorship contribution statement

Hamza Ibrahim: Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Methodology, Investigation, Formal analysis, Data curation, Conceptualization; **Love Allen Chijioke Ahakonye:** Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization; **Jae-Min Lee:** Validation, Supervision, Resources, Project administration, Funding acquisition, Formal analysis; **Dong-Seong Kim:** Writing – review & editing, Validation, Supervision, Resources, Project administration, Funding acquisition, Formal analysis, Conceptualization.

Data availability

No data was used for the research described in the article.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was partly supported by the Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government (MSIT) (IITP-2026-RS-2020-II201612, 25%), by the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 25%), and by the MSIT, Korea, under the ITRC support program (IITP-2026-RS-2024-00438430, 25%) and by the Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (RS-2026-25431637, 25%).

References

[1] E. Zeydan, C.D. Alwis, R. Khan, Y. Turk, A. Aydeger, T.R. Gadekallu, M. Liyanage, Quantum technologies for beyond 5G and 6G networks: applications, opportunities, and challenges, IEEE Open J. Commun. Soc. 6 (2025) 6383–6420. https://doi.org/10.1109/OJCOMS.2025.3591842

[2] L.A.C. Ahakonye, C.I. Nwakanma, J.-M. Lee, D.-S. Kim, Trees bootstrap aggregation for detection and characterization of IoT-SCADA network traffic, IEEE Trans. Ind. Inf. 20 (4) (2024) 5217–5228. https://doi.org/10.1109/TII.2023.3333438

[3] I.A. Sikiru, A.D. Kora, E.C. Ezin, A.L. Imoize, C.-T. Li, Hybridization of learning techniques and quantum mechanism for iiot security: applications, challenges, and prospects, Electron. (Basel) 13 (2024) (21). https://doi.org/10.3390/electronics13214153

[4] Y. Li, Y. Xiao, W. Liang, J. Cai, R. Zhang, K.-C. Li, M.K. Khan, The security and privacy challenges toward cybersecurity of 6G networks: a comprehensive review, Comput. Sci. Inform. Syst. 21 (3) (2024) 851–897. https://doi.org/10.2298/CSIS230804016L

[5] P. Bhattacharya, A. Kumari, S. Tanwar, I. Budhiraja, S. Patel, J.J. Rodrigues, Quant-jack: quantum machine learning to detect cryptojacking attacks in iiot networks, in: 2024 IEEE International Conference on Communications Workshops (ICC Workshops), 2024, pp. 865–870. https://doi.org/10.1109/ICCWorkshops59551.2024.10615371

[6] M. Hdaib, S. Rajasegarar, L. Pan, Quantum deep learning-based anomaly detection for enhanced network security, Quant. Mach. Intell. 6 (1) (2024) 26. https://doi.org/10.1007/s42484-024-00163-2

[7] P. Sharma, R. Singh, Blockchain-enabled secure frameworks for iiot in 6G networks, IEEE Internet Thing. J. 10 (4) (2023) 3201–3215. https://doi.org/10.1109/JIOT.2023.3245678

[8] H. Ibrahim, J. Kim, U.A. Bukar, Leveraging Blockchain technology for trustworthy information dissemination in Nigerian networks, J. Content. Comput. 5 (2) (2023) 727–753. https://doi.org/10.9728/jcc.2023.12.5.2.727

[9] M. Alazab, S. Khan, A. Rauf, Quantum machine learning meets Blockchain: a secure edge intelligence framework for 6G, Fut. Gener. Comput. Syst. 145 (2023) 1123–1136. https://doi.org/10.1016/j.future.2023.01.015

[10] A. Jahid, M.H. Alsharif, T.J. Hall, The convergence of Blockchain, iot and 6G: potential, opportunities, challenges and research roadmap, J. Netw. Comput. Applic. 217 (2023) 103677. https://doi.org/10.1016/j.jnca.2023.103677

[11] S. Cherbal, A. Zier, S. Hebal, L. Louail, B. Annane, Security in Internet of Things: a review on approaches based on Blockchain, machine learning, cryptography, and quantum computing, J. Supercomput. 80 (3) (2024) 3738–3816. https://doi.org/10.1007/s11227-023-05616-2

[12] T.Q. Duong, J.A. Ansere, B. Narottama, V. Sharma, O.A. Dobre, H. Shin, Quantum-inspired machine learning for 6G: fundamentals, security, resource allocations, challenges, and future research directions, IEEE Open J. Vehicul. Technol. 3 (2022) 375–387. https://doi.org/10.1109/OJVT.2022.3202876

[13] Y. Hu, Q. Jia, Y. Yao, Y. Lee, M. Lee, C. Wang, X. Zhou, R. Xie, F.R. Yu, Industrial Internet of Things intelligence empowering smart manufacturing: a literature review, IEEE Internet Thing. J. 11 (11) (2024) 19143–19167. https://doi.org/10.1109/JIOT.2024.3367692

[14] D. Mourtzis, N. Panopoulos, J. Angelopoulos, Chapter 5 - production management guided by Industrial Internet of Things and adaptive scheduling in smart factories, Elsevier, 2022. Design and Operation of Production Networks for Mass Personalization in the Era of Cloud Technology. https://doi.org/10.1016/B978-0-12-823657-4.00014-2

[15] H.V. Krishna, K.R. Sekhar, A study of Cybersecurity in Industrial Internet of Things (IIoT), Singapore, Springer Nature Singapore, 2024. Advances in Microelectronics, Embedded Systems and IoT. https://doi.org/10.1007/978-981-97-0767-6_43

[16] S.P. Singh, G. Piras, W. Viriyasitavat, E. Kariri, K. Yadav, G. Dhiman, S. Vimal, S.B. Khan, Cyber Security and 5G-assisted Industrial Internet of Things using Novel Artificial Adaption Based Evolutionary Algorithm, Mobile Networks and Applications, 2023. https://doi.org/10.1007/s11036-023-02230-7

[17] Z. Lei, J. Shi, Z. Luo, M. Cheng, J. Wan, Intelligent manufacturing from the perspective of industry 5.0: application review and prospects, IEEE Access 12 (2024) 167436–167451. https://doi.org/10.1109/ACCESS.2024.3496697

[18] W. Villegas-Ch, J.G.a. a Ortiz, S.S. a¡ nchez Viteri, Toward intelligent monitoring in iot: AI applications for real-time analysis and prediction, IEEE Access 12 (2024) 40368–40386. https://doi.org/10.1109/ACCESS.2024.3376707

[19] P. Bhide, D. Shetty, S. Mikkili, Review on 6G communication and its architecture, technologies included, challenges, security challenges and requirements, applications, with respect to AI domain,, IET Quant. Commun. 6 (1) (2025) 12114. https://doi.org/10.1049/qtc2.12114

[20] A. Goudarzi, F. Ghayoor, M. Waseem, S. Fahad, I. Traore, A survey on iot-enabled smart grids: emerging, applications, challenges, and outlook, Energies 15 (19). https://doi.org/10.3390/en15196984

[21] A.A. Mirani, G. Velasco-Hernandez, A. Awasthi, J. Walsh, Key challenges and emerging technologies in industrial iot architectures: a review, Sensors 22 (2022) (15). https://doi.org/10.3390/s22155836

[22] S.S. Albouq, A.A.A. Sen, N. Almashf, M. Yamin, A. Alshanqiti, N.M. Bahbouh, A survey of interoperability challenges and solutions for dealing with them in iot environment, IEEE Access 10 (2022) 36416–36428. https://doi.org/10.1109/ACCESS.2022.3162219

[23] L.A.C. Ahakonye, C.I. Nwakanma, D.-S. Kim, Tides of Blockchain in IoT cybersecurity, Sensors 24 (10) (2024) 3111. https://doi.org/10.3390/s24103111

[24] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, S. Lloyd, Quantum machine learning, Nature 549 (7671) (2017) 195–202. https://doi.org/10.1038/nature23474

[25] M. Schuld, N. Killoran, Quantum machine learning in feature Hilbert spaces, Phys. Rev. Lett. 122 (4) (2019). https://doi.org/10.1103/PhysRevLett.122.040504

[26] K. Dave, N. Innan, B.K. Behera, S. Mumtaz, S. Al-Kuwari, A. Farouk, Optimizing low-energy carbon IIoT systems with quantum algorithms: performance evaluation and noise robustness, IEEE Internet Thing. J. 12 (17) (2025) 34653–34662. https://doi.org/10.1109/JIOT.2025.3540949

[27] A.R. L. D.M. aªdo, S.K. Jagatheesaperumal, K.A. P.D. Costa, K. Acharya, H. Song, M. Guizani, V.H. C.D. Albuquerque, Quantum ai-enhanced IoT-fog communication: a survey from cybersecurity and data privacy perspective, 2025, pp. 1. https://doi.org/10.1109/COMST.2025.3622378

[28] M.Y. Küçükkara, F. Atban, C.B. lmış, Quantum-neural network model for platform independent ddos attack classification in cyber security, Adv. Quant. Technolog. 7 (10) (2024) 2400084. https://doi.org/10.1002/qute.202400084

[29] V. Rishiwal, U. Agarwal, M. Yadav, S. Tanwar, D. Garg, M. Guizani, A new alliance of machine learning and quantum computing: concepts, attacks, and challenges in IoT networks, IEEE Internet Thing. J. 12 (12) (2025) 18865–18886. https://doi.org/10.1109/JIOT.2025.3535414

[30] S. Pirandola, U.L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J.M. Arrazola, J.S. Sidhu, K. Tamaki, W. Wang, C. Weedbrook, Advances in quantum cryptography, Adv Opt Photon. 12 (4) (2020) 1012–1236. https://doi.org/10.1364/AOP.361502

[31] S. Jerbi, V. Savona, G. Carleo, P.D. Karagiannidis, Quantum reinforcement learning: the state of the art, Mach. Learn.: Sci. Technol. 2 (3) (2021). https://doi.org/10.1088/2632-2153/abef86

[32] K. Gupta, P. Jahnavi, A. Hazra, A. Bablani, Quantum Machine Learning for Industry 5, 0, Springer, 2025. https://doi.org/10.1007/978-3-031-87837-4_7

[33] A.E. Azzaoui, M.M. Salim, J.H. Park, Secure and reliable big-data-based decision making using quantum approach in IIoT systems, Sensors 23 (2023) (10). https://doi.org/10.3390/s23104852

[34] P. Lamichhane, D.B. Rawat, Quantum machine learning: recent advances, challenges, and perspectives, IEEE Access 13 (2025) 94057–94105. https://doi.org/10.1109/ACCESS.2025.3573244

[35] S.K. Sood, M. Singh, M. Bhatia, Industrial progress with quantum algorithms: an in-depth review, J. Supercomput. 81 (2025) 1064. https://doi.org/10.1007/s11227-025-07555-6

[36] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.(2020)

[37] A. Javadpour, A.K. Sangaiah, W. Zhang, et al., Decentralized ai-based task distribution on Blockchain for cloud industrial Internet of Things, J. Grid Comput. 22 (2024) 33. https://doi.org/10.1007/s10723-024-09751-9

[38] Y. Bobde, G. Narayanan, M. Jati, R.S.P. Raj, I. Cvitiä‡, D. Perakoviä‡, Enhancing industrial IoT network security through Blockchain integration, Electron. (Basel) 13 (2024) (4). https://doi.org/10.3390/electronics13040687

[39] A. Meydani, H. Shahinzadeh, A. Ramezani, M. Moazzami, H. Nafisi, H. Askarian-Abyaneh, State-of-the-art analysis of Blockchain-based industrial IoT (IIoT) for smart grids, in: 2024 9th International Conference on Technology and Energy Management (ICTEM), 2024, pp. 1–12. https://doi.org/10.1109/ICTEM60690.2024.10631931

[40] P.M. Chanal, M.S. Kakkasageri, Blockchain-based data integrity framework for Internet of Things, Int. J. Inf. Secur. 23 (2024) 519–532. https://doi.org/10.1007/s10207-023-00719-6
[41] N. Xiao, Z. Wang, X. Sun, J. Miao, A novel Blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things, Alexandr. Eng. J. 86 (2024) 631–643. https://doi.org/10.1016/j.aej.2023.12.021
[42] D. Li, H. Li, N. Crespi, R. Minerva, M. Li, W. Liang, K.-C. Li, Hyper-IIoT: a smart contract-inspired access control scheme for resource-constrained industrial Internet of Things, IEEE Trans. Sustain. Comput. 10 (5) (2025) 820–829. https://doi.org/10.1109/TSUSC.2025.3542466
[43] A. Umar, D. Kumar, T. Ghose, T.A.H. Alghamdi, A.Y. Abdelaziz, Decentralized community energy management: enhancing demand response through smart contracts in a Blockchain network, IEEE Access 12 (2024) 80781–80798. https://doi.org/10.1109/ACCESS.2024.3409706
[44] N. Zeng, X. Ye, S. Chen, Y. Liu, Q. Li, Transforming modular construction supply chains: integrating smart contracts and robotic process automation (RPA) for enhanced coordination and automation, Appl. Sci. 15 (21). https://doi.org/10.3390/app152111670
[45] M. Usman, M.S. Sarfraz, M.U. Aftab, U. Habib, S. Javed, A Blockchain based scalable domain access control framework for industrial Internet of Things, IEEE Access 12 (2024) 56554–56570. https://doi.org/10.1109/ACCESS.2024.3390842
[46] T.A. Alghamdi, R. Khalid, N. Javaid, A survey of Blockchain based systems: scalability issues and solutions, applications and future challenges, IEEE Access 12 (2024) 79626–79651. https://doi.org/10.1109/ACCESS.2024.3408868
[47] J.C. Ferreira, Bridging the gaps: future directions for Blockchain and IoT integration in smart grids, Energies 18 (4). https://doi.org/10.3390/en18040772
[48] P. Maiti, S. Prabhu, P. Ashok, Decentralized defenses: a framework for 5G IoT security in industry 4.0 using Blockchain crowdsourcing, in: 2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL), (2024), pp. 534–538. https://doi.org/10.1109/ICSADL61749.2024.00093
[49] O. Popoola, M. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehai, J. Popoola, A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & Blockchain: problems, challenges and solutions, Blockchain: Res. Applic. 5 (2) (2024) 100178. https://doi.org/10.1016/j.bcra.2023.100178
[50] F.A. Alaba, H.A. Sulaimon, M.I. Marisa, O. Najeem, Smart contracts security application and challenges: a review, Cloud Comput. Data Sci. 5 (1) (2024) 15–41. https://doi.org/10.37256/ccds.5120243271
[51] C.R. A, A.K. Pani, P. Kumar, Blockchain-enabled smart contracts and the internet of things: advancing the research agenda through a narrative review, Multimed. Tool. Appl. 84 (2025) 5097–5147. https://doi.org/10.1007/s11042-024-18931-4
[52] K. Wimal, G. Liyanage, A truly decentralized Blockchain consensus protocol that avoids concentration of power, in: 2023 IEEE 17th International Conference on Industrial and Information Systems (ICIIS), 2023, pp. 1–6. https://doi.org/10.1109/ICIIS58898.2023.10253613
[53] M.M. Islam, M.M. Merlec, H.P. In, Proof of random leader: a fast and manipulation-resistant proof-of-authority consensus algorithm for permissioned Blockchains using verifiable random function, IEEE Trans. Serv. Comput. 18 (3) (2025) 1655–1668. https://doi.org/10.1109/TSC.2025.3536315
[54] D.-S. Kim, I.S. Igboanusi, L.A.C. Ahakonye, G.O. Anyanwu, Proof-of-authority-and-association consensus algorithm for IoT Blockchain networks, in: 2025 IEEE International Conference on Consumer Electronics (ICCE), 2025, pp. 1–6. https://doi.org/10.1109/ICCE63647.2025.10930052
[55] A. Ninkov, J.R. Frank, L.A. Maggio, Bibliometrics: methods for studying academic publishing, Perspect. Med. Educ. 11 (3) (2022) 173–176. https://doi.org/10.1007/s40037-021-00695-4
[56] U. Bello, H. Adamu, S. Samsuri, H. Ibrahim, M. Qamar, Improving biodiesel oxidative stability using antioxidants: an insight into the research trends and future prospects from a bibliometric approach, Result. Eng. 26 (2025) 105185. https://doi.org/10.1016/j.rineng.2025.105185
[57] J.B.-W. ny, M.S. gowski, A comprehensive bibliometric analysis of business process management and knowledge management integration: bridging the scholarly gap, Information 15 (8). https://doi.org/10.3390/info15080436
[58] A.Y. Nageye, A.D. Jimale, M.O. Abdullahi, Y.A. Ahmed, Emerging trends in data science and big data analytics: a bibliometric analysis, Int. J. Electron. Commun. Eng. 11 (5) (2024) 84–98. https://doi.org/10.14445/23488549/IJECE-V11I5P109
[59] A. Bashar, M. Wasiq, B. Nyagadza, E.T. Maziriri, Emerging trends in social media marketing: a retrospective review using data mining and bibliometric analysis, Fut. Bus. J. 10 (1) (2024) 23. https://doi.org/10.1186/s43093-024-00308-6
[60] J.Y. Lee, S.Y. Syn, S. Kim, Global research trends in research data management: a bibliometrics approach, J. Librariansh. Inform. Sci. 57 (3) (2025) 719–732. https://doi.org/10.1177/09610006241239083
[61] C. Dindorf, E. Bartaguiz, F. Gassmann, M. Fröhlich, Conceptual structure and current trends in artificial intelligence, machine learning, and deep learning research in sports: a bibliometric review, Int. J. Environ. Res. Public Health 20 (1) (2022) 173. https://doi.org/10.3390/ijerph20010173
[62] U.A. Bukar, M.S. Sayeed, S.F.A. Razak, S. Yogarayan, O.A. Amodu, R.A.R. Mahmood, A method for analyzing text using vosviewer, MethodsX 11 (2023) 102339. https://doi.org/10.1016/j.mex.2023.102339
[63] D. Budgen, P. Brereton, Performing systematic literature reviews in software engineering, in: Proceedings of the 28th International Conference on Software Engineering, ICSE '06, the 28th International Conference on Software Engineering, ICSE '06New York, NY, USA, Association for Computing Machinery, 2006, p. 1052. https://doi.org/10.1145/1134285.1134500
[64] C.D.L. Cruz-Lovera, A.J. Perea-Moreno, J.L. D.L. Cruz-Fernandez, F.G. Montoya, A. Alcayde, F. Manzano-Agugliaro, Analysis of research topics and scientific collaborations in energy saving using bibliometric techniques and community detection, Energies 12. https://doi.org/10.3390/en12102030
[65] Z.A. Polat, M. Alkan, J. Paulsson, J.M. Paasch, E. Kalogianni, Global scientific production on ladm-based research: a bibliometric analysis from 2012 to 2020, Land Use Policy 112 (2022) 105847. https://doi.org/10.1016/j.landusepol.2021.105847
[66] N.J.V. Eck, L. Waltman, Vosviewer: a computer program for bibliometric mapping, Scientometrics 84 (2) (2010) 523–538. https://doi.org/10.1007/s11192-010-0201-2
[67] A. Perianes-Rodriguez, L. Waltman, N.J.V. Eck, Mapping the structure of knowledge in the field of bibliometrics, J. Informetr. 10 (3) (2016) 713–725. https://doi.org/10.1016/j.joi.2016.06.002
[68] N.J.V. Eck, L. Waltman, Software survey: vosviewer, a computer program for bibliometric mapping, Scientometrics 84 (2) (2010) 523–538. https://doi.org/10.1007/s11192-009-0146-3
[69] W. Yun, J. Kim, S. Jung, J. Kim, J. Kim, Quantum multiagent actor-critic neural networks for internet-connected multirobot coordination in smart factory management, IEEE Internet Thing. J. 10 (2023) 9942–9952. https://doi.org/10.1109/JIOT.2023.3234911
[70] M. Peelam, A. Rout, V. Chamola, Quantum computing applications for Internet of Things. https://doi.org/10.1049/qtc2.12079
[71] A. Melnikov, M. Kordzanganeh, A. Alodjants, R. Lee, Quantum Machine Learning: from physics to software engineering, Adv. Phys.: X 8, https://doi.org/10.1080/23746149.2023.2165452
[72] X. Hua, D. Li, Y. Fu, Y. Zhu, Y. Jiang, J. Zhou, X. Yang, Y. Tan, in: Hierarchical Controlled Hybrid Quantum Communication Based on Six-Qubit Entangled States in IoT, Basel, Switzerland,(2023) p. 23. https://doi.org/10.3390/s23229111
[73] S.K. Satpathy, V. Vibhu, B.K. Behera, S. Al-Kuwari, S. Mumtaz, A. Farouk, Analysis of Quantum Machine Learning algorithms in noisy channels for classification tasks in the IoT extreme environment, IEEE Internet Thing. J. 11 (3) (2023) 3840–3852. https://doi.org/10.1109/JIOT.2023.3300577
[74] S.S. Gill, Quantum and Blockchain based serverless edge computing: a vision, model, new trends and future directions, Internet Technol. Lett. 7 (1) (2024) 275. https://doi.org/10.1002/itl2.275
[75] B. Narottama, Z. Mohamed, S.A. Aïssa, Quantum machine learning for next-g wireless communications: fundamentals and the path ahead, IEEE Open J. Commun. Soc. 4 (2023) 2204–2224. https://doi.org/10.1109/OJCOMS.2023.3309268
[76] H. Cao, S. Garg, S. Mumtaz, M. Alrashoud, L. Yang, G. Kaddoum, Softwarized resource allocation in digital twins-empowered networks for future quantum-enabled consumer applications, IEEE Trans. Consum. Electron. 70 (1) (2024) 800–810. https://doi.org/10.1109/TCE.2024.3370052
[77] S. Kundu, S. Ghosh, Security Aspects of Quantum Machine Learning: Opportunities, Threats and Defenses, New York, NY, USA, Association for Computing Machinery, 2022. Proceedings of the Great Lakes Symposium on VLSI 2022, GLSVLSI '22. https://doi.org/10.1145/3526241.3530833
[78] V.-L. Nguyen, L.-H. Nguyen, R.-H. Hwang, B. Canberk, T.Q. Duong, Quantum Machine Learning for 6G network intelligence and adversarial threats, IEEE Commun. Stand. Maga. 9 (3) (2025) 40–48. https://doi.org/10.1109/MCOMSTD.2025.3575261
[79] Y. Li, Y. Zuo, H. Song, Z. Lv, Deep learning in security of Internet of Things, IEEE Internet Thing. J. 9 (2022) 22133–22146. https://doi.org/10.1109/JIOT.2021.3106898

[80] F. Saleh, A. Al-Fuqaha, Dag-based Blockchain for industrial IoT: performance and security analysis, IEEE Trans. Ind. Inf. 17 (6) (2021) 4204–4213. https://doi.org/10.1109/TII.2021.3054567
[81] Z. Xu, W. Zhang, Energy-efficient proof-of-stake Blockchain for IIoT applications, Sensors 22 (3) (2022) 1124. https://doi.org/10.3390/s22031124
[82] A. Lahbib, K. Toumi, A. Laouiti, S. Martin, Blockchain based distributed trust management in IoT and IIoT: a survey, J. Supercomput. 80 (2024) 21867–21919. https://doi.org/10.1007/s11227-024-06286-4
[83] M.A. Obaidat, M. Rawashdeh, M.A. ™afreh, M. Abouali, K. Thakur, A. Karime, Exploring IoT and Blockchain: a comprehensive survey on security, integration strategies, applications and future research directions, Big Data Cogn. Comput. 8 (12) (2024) 174. https://doi.org/10.3390/bdcc8120174
[84] F.G. Ghajar, A. Sikora, D. Welte, Schloss: Blockchain-based system architecture for secure industrial IoT, Electron. (Basel) 11 (10) (2022) 1629.
[85] S. Asaithambi, S. Nallusamy, J. Yang, S. Prajapat, G. Kumar, P.S. Rathore, A Secure and Trustworthy Blockchain-Assisted Edge Computing Architecture for Industrial Internet of Things, https://doi.org/10.1007/s41598-025-00337-3
[86] L. Gong, D.M. Alghazzawi, L. Cheng, Bcot sentry: a Blockchain-based identity authentication framework for IoT devices, Inform. (Basel) 12 (5) (2021) 203. https://doi.org/10.3390/info12050203
[87] S. Almarri, A. Aljughaiman, Blockchain technology for IoT security and trust: a comprehensive slr, Sustainability 16 (23) (2024) 10177. https://doi.org/10.3390/su162310177
[88] D. Wu, N. Ansari, A trust-evaluation-enhanced Blockchain-secured industrial IoT system, IEEE Internet Thing. J 8 (8) (2020) 5510–5517. https://doi.org/10.1109/JIOT.2020.2982424
[89] M.S. Al-Rakhami, M. Al-Mashari, A Blockchain-based trust model for the internet of things supply chain management, Sensors 21 (5) (2021) 1759. https://doi.org/10.3390/s21051759
[90] P. Vern, A. Panghal, R.S. Mor, V. Kumar, S. Jagtap, Blockchain-based traceability framework for agri-food supply chain: a proof-of-concept, Oper. Manage. Res. 18 (2) (2025) 554–573. https://doi.org/10.1007/s12063-024-00529-6
[91] H. Ibrahim, K.J. Mukisa, L.A.C. Ahakonye, J.M. Lee, D.-S. Kim, Impact of purechain for secure and scalable cybersecurity in resource-constrained IIoT, Proceedings of the 35th Joint Conference on Communications and Information 2025 (2025) 1–2.
[92] N.S. Sizan, D. Dey, M.A. Layek, M.A. Uddin, E.-N. Huh, Evaluating Blockchain Platforms for IoT Applications in Industry 5.0: A Comprehensive Review 6 (2025) 100276. https://doi.org/10.1016/j.bcra.2025.100276
[93] V. Buterin, A next-generation smart contract and decentralized application platform, 2014. https://ethereum.org/whitepaper.
[94] Z. Zheng, S. Xie, H.N. Dai, X. Chen, Blockchain challenges and opportunities: a survey, Int. J. Web Grid Serv. 13 (4) (2017) 224–237. https://doi.org/10.1504/IJWGS.2017.087032
[95] F. Arute, et al., Quantum supremacy using a programmable superconducting processor, Nature 574 (7779) (2019) 505–510. https://doi.org/10.1038/s41586-019-1666-5
[96] Y. Zhang, H. Chen, Blockchain-based secure data sharing and storage in IoT, IEEE Internet Thing. J. 6 (3) (2019) 4660–4669.
[97] A.E. Gencer, et al., Decentralized Blockchain in IIoT: a survey, IEEE Internet Thing. J. 5 (3) (2018) 2275–2287. https://doi.org/10.1109/JIOT.2018.2868547
[98] J. Pan, L. Zhang, Blockchain-based trust management in the internet of things, J. Netw. Comput. Applic. 163 (2020) 102709. https://doi.org/10.1016/j.jnca.2020.102709
[99] L. Xu, L. Chen, Z. Gao, Blockchain in industrial IoT: challenges and solutions, IEEE Internet Thing. J. 5 (6) (2018) 5310–5320. https://doi.org/10.1109/JIOT.2018.2874464
[100] G. Zyskind, O. Nathan, A. Pentland, Decentralizing Privacy: Using Blockchain to Protect Personal Data, IEEE Security and Privacy Workshops, 2015. https://doi.org/10.1109/SPW.2015.27
[101] R. Kumar, R. Tripathi, H. Gupta, Blockchain-enabled security for IoT devices, IEEE Consum. Electron. Mag. 9 (2) (2020) 45–49. https://doi.org/10.1109/MCE.2019.2953727
[102] W. Zhang, M. Li, F. Wang, Quantum-inspired resource optimization for 6G networks, IEEE Internet Thing. J. 12 (3) (2025) 2011–2029. https://doi.org/10.1109/JIOT.2025.3087654
[103] L. Chen, R. Zhao, Q. Huang, Digital twins in the IIoT: integration of Blockchain and ai, Digit. Transform. 18 (5) (2025) 877–891.
[104] A. Patel, S. Kumar, R. Singh, Smart grid control: adaptive Blockchain and quantum ml approaches, J. Ind. IoT Syst. 10 (4) (2024) 349–365. https://doi.org/10.3786/jiots.2024.1004
[105] J. Kim, S. Park, T. Lin, Federated learning and Blockchain for scalable IIoT in 6G, IEEE Trans. Netw. Sci. Eng. 11 (2) (2025) 334–347. https://doi.org/10.1109/TNSE.2025.3121345
[106] C.I. Okafor, L.A.C. Ahakonye, J.M. Lee, D.-S. Kim, Purequantum: towards a scalable Blockchain channel security in IoI networks, 2025, p. 100372. https://doi.org/10.1016/j.bcra.225.100372
[107] C. Lee, F. Wang, K. Sen, Blockchain-enabled secure management for IIoT: prototyping and validation, IEEE Internet Thing. J. 11 (7) (2024) 6312–6330. https://doi.org/10.1109/JIOT.2024.3071650