

Convergence of blockchain, IoT, and machine learning: exploring opportunities and challenges – a systematic review

Youssef Aounzou^{1,*},
Abdelhak Boulaalam¹ and
Fahd Kalloubi^{2,3}

¹LSI Laboratory, National Schools
of Applied Sciences, Sidi Mohamed
Ben Abdellah University, Fez,
Morocco

²Mohammed VI Polytechnic
University UM6P, Vanguard Center,
Benguerir, Morocco

³LTI Laboratory, National School
of Applied Sciences, Chouaib
Doukkali University of El Jadida,
El Jadida, Morocco

Contributing authors: kalloubi.f@
ucd.ac.ma (Fahd Kalloubi); abdel-
hak.boulaalam@usmba.ac.ma
(Abdelhak Boulaalam)

*E-mail: youssef.aounzou@usmba.
ac.ma

Received for publication
November 17, 2024.

Abstract

With the rapid technological advancement, the convergence of the Internet of Things (IoT), blockchain, and machine learning (ML) has a significant revolution across industries, driving them in areas like Industry 4.0, smart cities, and advanced transportation systems. This study presents a comprehensive review of the integration of the IoT, blockchain, and ML technologies, highlighting their transformative impact on diverse industries. It addresses the challenges of scalability, security, and data management posed by the growth of interconnected IoT devices, proposing solutions through advanced algorithms and the integration of blockchain for data security and immutability. By examining real-world applications and reviewing existing literature, this study underscores the potential benefits and complexities of merging these technologies, while also identifying research challenges and future directions. Overall, it offers insights into the innovative constructive collaboration of IoT, blockchain, and ML, which has become the most important of modern technological advances.

Keywords

blockchain, Internet of things, machine learning, artificial intelligence

I. Introduction

I.1 Significance of blockchain, IoT, and ML technologies

Over the past 10 years, the combination of the Internet of Things (IoT), blockchain, and machine learning (ML) has brought about significant changes in various industries. This convergence has led to groundbreaking advances in industries, such as Industry 4.0, smart cities, smart tourism, and transportation systems. However, the extensive usage of IoT devices has also posed significant challenges in terms of scalability, security, privacy, and data

management, due to the ever-growing number of interconnected devices. This ongoing proliferation of networked devices contributes to complexity, as each element has networking capabilities that enable the exchange and collection of information both locally and remotely over the Internet. As IoT systems communicate primarily over the Internet, their inherent vulnerability to a wide range of security risks becomes increasingly apparent [1]. This underscores the need for robust security measures to protect the integrity and confidentiality of data within these interconnected systems. To meet this requirement, it is necessary to deploy advanced algorithms, ML models, and data analysis tools to efficiently navigate and extract

valuable information from an ever-changing data environment. Thus, the integration becomes imperative to guarantee the all-important aspects of data security, transparency, and immutability. Blockchain's decentralized and tamper-proof nature offers a solution to the security challenges inherent in traditional centralized systems, providing a secure foundation for the exchange and management of sensitive data within the rapidly expanding IoT ecosystem.

In the context of IoT applications, ML has evolved as a formidable tool for understanding models and facilitating real-time decision-making. Nonetheless, the security and privacy concerns linked to centralized ML frameworks have instigated an exploration of decentralized frameworks, with blockchain technology (BCT) assuming a critical role in this paradigm shift.

The incorporation of BCT enables not only the resolution of complex security and confidentiality challenges associated with automatic learning but also the improvement of the global performance of automatic learning algorithms by providing a reliable and secure database [2]. This mutually beneficial relationship between blockchain and ML has the potential to have a revolutionary impact on the global economy by introducing transformative changes in how data are handled, secured, and used to make strategic decisions. Aside from its capabilities in the resolution of security issues, blockchain establishes a sturdy framework that is invaluable for storing complete records of various activities and decisions in the field of IoT applications. This combined functionality enhances both data exchange efficiency and reliability while fostering continuous innovation in IoT. The confluence of blockchain and automatic learning strengthens not only the foundations of secure data practices but also propels a wave of innovation and development in the interconnected IoT environment.

As detailed in several reviews [2–8], the combination of IoT, blockchain, and ML technology offers considerable potential for improving algorithm performance and guaranteeing prediction accuracy. Indeed, data stored on a blockchain network is invulnerable to manipulation and error, reducing the risk of introducing errors or biases into ML models.

This study aims to comprehensively analyze the complex integration of IoT, blockchain, and ML technologies across various fields, exploring their potential applications and emphasizing the transformative power of their combined synergy. It also examines real-world scenarios and applications, revealing the complexities of integrating these technologies and illustrating how they can work together to assist

industries, such as Industry 4.0, smart factories, smart tourism, and advanced transportation systems. Furthermore, it delves into the challenges associated with merging these disparate technologies, focusing on security, privacy, and data management issues. Simultaneously, the study identifies and explores the numerous opportunities presented by their seamless integration, offering a forward-looking perspective on potential innovations and improvements in a rapidly evolving technology landscape.

Compared to existing reviews, this study provides a valuable roadmap for understanding the opportunities and challenges related to IoT integration, blockchain, and ML. It combines a comprehensive review of existing research with real-world applications, including case studies from supply chain management, healthcare, smart cities, and renewable energy, demonstrating the practical impact of these technologies. This study also identifies crucial areas for future research, focusing on challenges such as data complexity, scalability, security, explainability, and regulatory frameworks, highlighting priorities for future development to fully realize the potential of these technologies.

1.2 Review method

To ensure a comprehensive and accurate analysis, an efficient review process has been implemented, as illustrated in Figure 1. Initially, a search was conducted using relevant keywords such as “AI,” “IoT,” and “blockchain,” which resulted in a collection of 130 articles. This initial pool of articles covered a broad spectrum of research within these fields.

The next step involved removing duplicate entries, which refined the set to 74 unique research papers. This crucial step ensured that each piece of research considered in the analysis was distinct and contributed uniquely to the understanding of the intersection of Artificial Intelligence (AI), IoT, and blockchain.

Subsequently, the abstracts of these 74 papers were meticulously reviewed. This review process was essential for determining the relevance of each article to the specific intersection of AI, IoT, and blockchain technologies. Articles that did not directly address the integration or application of these three technologies were excluded from further consideration. This careful curation resulted in a final selection of 64 research publications that were deemed most relevant for an in-depth review.

Figure 2 provides a detailed breakdown of the selected articles by topic, further highlighting the focus

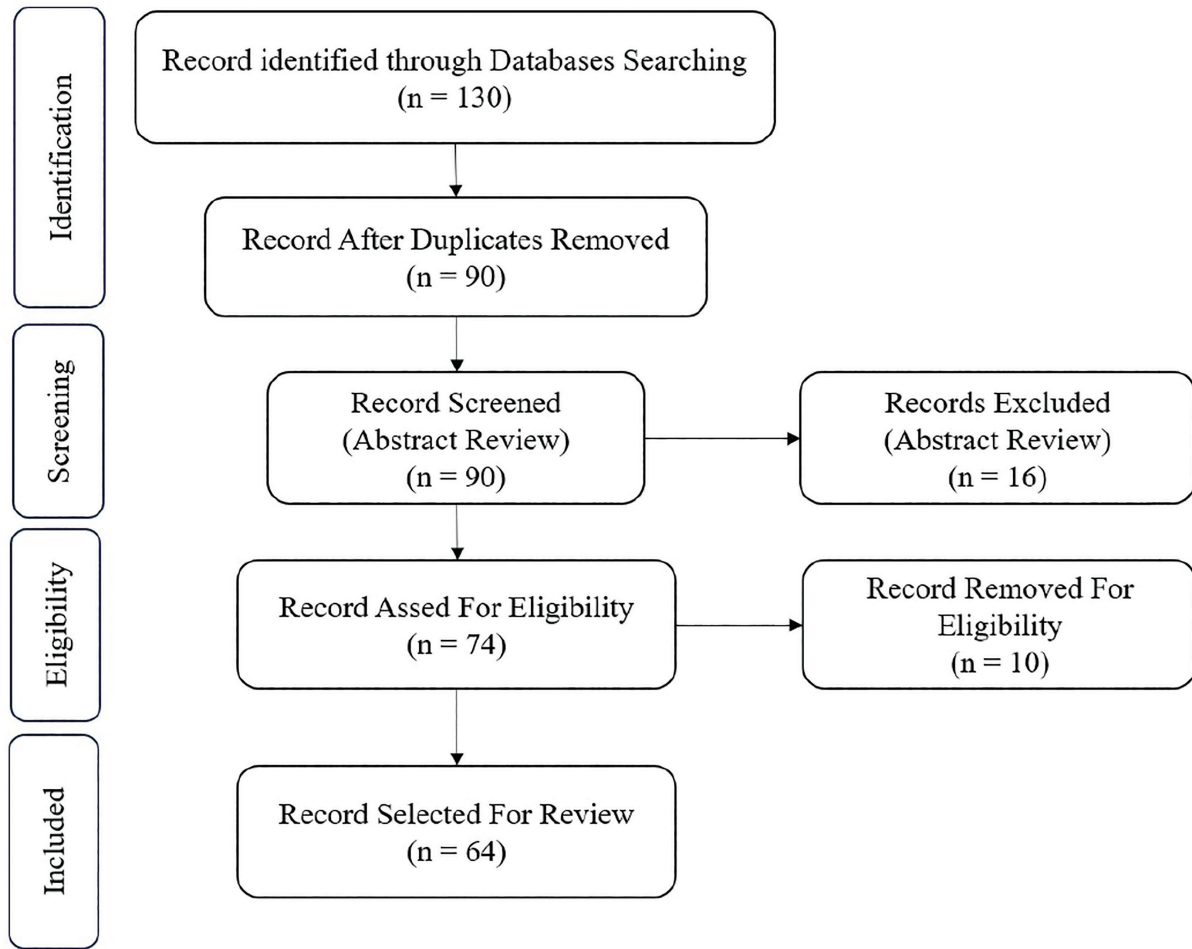


Figure 1: Research methodology.

areas of the research. This systematic categorization of articles ensured a clear understanding of the specific domains within AI, IoT, and blockchain where significant research contributions have been made. For instance, some articles focused on the application of blockchain to enhance security in IoT networks, while others explored the use of AI for predictive maintenance in IoT devices.

This systematic approach not only ensured the inclusion of the most relevant and recent research but also facilitated a comprehensive understanding of how these technologies are being integrated across diverse fields. Through critical selection and organization of research, we provided a nuanced view of current advancements, identified emerging trends, and pinpointed areas for further exploration. This methodical process underscores the importance of a rigorous review in synthesizing a vast body of literature into coherent and insightful findings.

1.3 Organizations of the survey

The survey is structured as follows. Section 2 provides an overview of existing survey articles, emphasizing the unique contributions and distinctions of this study. Section 3 introduces foundational concepts related to ML, IoT, and blockchain. Subsequent sections explore blockchain applications in IoT frameworks (Section 4), IoT and AI applications (Section 5), blockchain and AI integration (Section 6), and the combined applications of blockchain and AI with IoT architectures (Section 7). Section 8 identifies crucial research challenges for future exploration, while Section 9 concludes by summarizing the key findings and offering insights into the potential of this convergence for developing intelligent and secure IoT systems.

The overall structure of this study is illustrated in Figure 3.

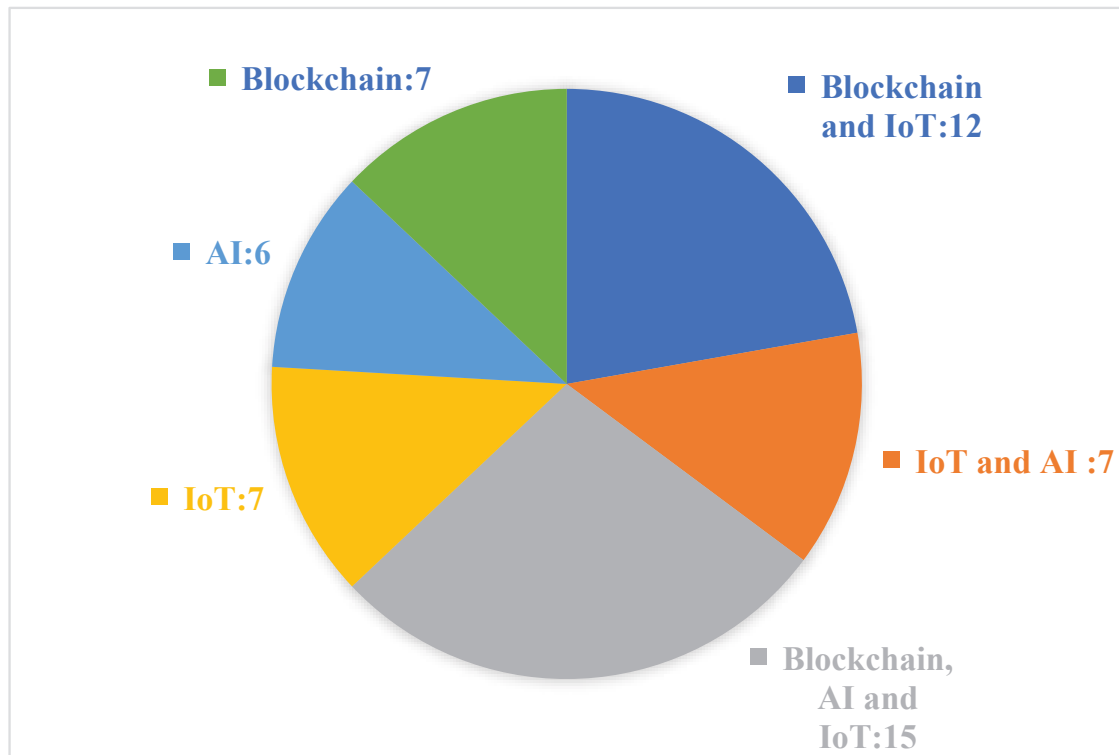


Figure 2: Elements percentile review. IoT, Internet of things.

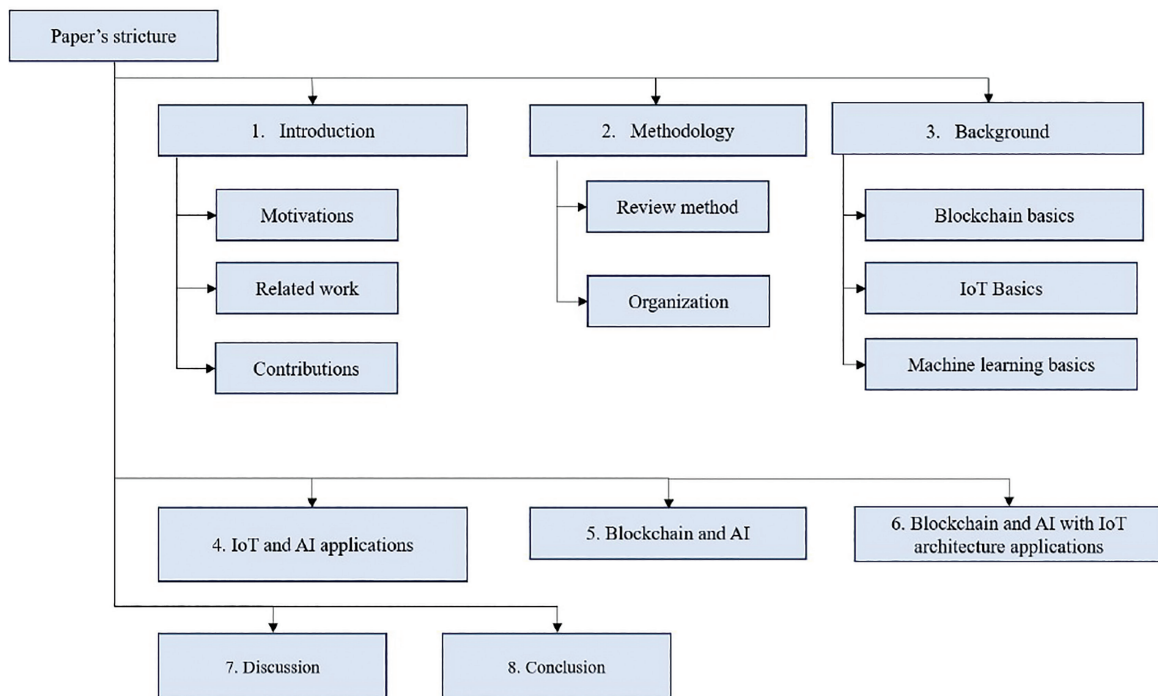


Figure 3: Study organization. AI, Artificial Intelligence; IoT, Internet of things.

To ensure clarity and consistency, Table 1 presents a comprehensive list of notations and their definitions used throughout this article.

II Literature review

II.1 Related work

Several reviews have been conducted to explore the integration of IoT, blockchain, and ML to enhance the security, scalability, and intelligence of IoT-based models. For example, a previous study [4] provides a comprehensive overview of various IoT, blockchain, and ML applications in the construction industry. The authors address challenges

in productivity, time management, effectiveness, and quality and attribute these issues to limited awareness of contemporary technologies prevalent in other disciplines. Likewise, another study on the field of smart healthcare provides insights into the challenges and opportunities of integrating these technologies into healthcare [8]. Additionally, research [2] analyzes using BCT as a framework for storing records of various activities and decisions in the context of IoT. Furthermore, existing research discusses the integration of IoT with BCT and AI technologies and highlights the potential synergies and impacts of such integration [3]. Based on this context, Table 2 provides an overview of the related review works in several fields, offering a comprehensive examination on how the integration of IoT, blockchain, and AI has been explored and analyzed in existing literature.

Table 1: List of acronyms used in this article

Acronym	Explanation
IoT	Internet of Things
BCT	Blockchain Technology
ML	Machine Learning
AI	Artificial Intelligence
SVM	Support Vector Machines
ANN	Artificial Neural Networks
IoMT	Internet of Medical Things
DL	Deep Learning
ANN	Artificial Neural Networks
DCDM	Decentralized IoT Collectability Data Marketplace
IDM	IoT Data Marketplace
P2P	Peer-To-Peer Model
PKI	Public Key Infrastructure
BloMTAKE	Blockchain-based IoMT Authenticated Key Exchange
IDS	Intrusion Detection Systems
GA	Genetic Algorithm
DA	Decision Tree Algorithm
LWAMCNet	Lightweight Automatic Modulation Classification Network
CKD	Chronic kidney disease
NormaChain	Blockchain-based normalized autonomous transaction settlement system
MTBF	Mean Time Between Failure
KPIs	Key Performance Indicators

II.2 Comparative analysis and motivational insights

Our review presents several distinctive strengths in comparison with existing works in the field of IoT, blockchain, and AI integration. While some research, such as the one on blockchain and AI integration in IoT [3], explores the potential benefits and challenges of this combination, our study goes further by providing a detailed analysis of specific synergies and proposing concrete solutions to overcome the identified challenges. Furthermore, while some studies (e.g., [9]) focus on security challenges using ML, AI, and BCT technologies, our contribution stands out by an in-depth analysis of standardized security protocols and advanced cryptographic methods.

Furthermore, our research differentiates itself by an in-depth analysis of interoperability aspects, proposing frameworks for smoother integration between these technologies, unlike a previous study [7] that focuses on overall technical challenges. Furthermore, our study proposes practical solutions to overcome the limitations of scalability and scalable blockchain architectures specific to IoT.

While the review [11] offers a comprehensive taxonomy and analysis of the challenges and opportunities in integrating blockchain and decentralized AI for cybersecurity, our study proposes concrete solutions for scalability and security challenges, as well as policy recommendations for responsible deployment of these technologies.

We do not limit ourselves to a single specific domain, but extend our analysis to various sectors.

Table 2: List of related review works

Reference	Year	Topic of review	Contribution
[3]	2023	Integration of blockchain and AI in the IoT	Explores how blockchain and AI can be used to improve the performance of IoT systems. Focuses on the potential benefits, limitations, challenges, and future research directions in this emerging field.
[9]	2020	Security challenges and solutions in IoT: A review of ML, AI, and blockchain integration	Addresses security challenges in IoT through systematic study of ML, AI, and BCT technologies.
[7]	2024	Convergence of IoT with blockchain and ML: Overview and challenges	Provides a comprehensive overview of the convergence of IoT with blockchain and ML algorithms, addressing technical challenges such as architecture, hardware, privacy and security, scalability, interoperability, and heterogeneity issues.
[10]	2024	Integration of edge computing and blockchain into IoT: Challenges and opportunities	Conducts a review of the integration of edge computing and blockchain into IoT systems, covering aspects of system architectures, categories of blockchain-based edge deployment, security requirements, and potential applications. Discusses challenges and insights into the future directions of blockchain-based edge IoT systems.
[11]	2024	Integration of blockchain with decentralized AI for cybersecurity: A systematic literature review	Offers a systematic literature review on the integration of BCT with decentralized AI within cybersecurity, providing a comprehensive taxonomy, analyzing the challenges and opportunities, and discussing real-world applications and future research directions.
[12]	2024	Integration of AI, IoT, Blockchain, and Nanotechnology in Colorectal Cancer Diagnosis and Treatment	Discusses the potential of integrating advanced technologies to improve diagnostic accuracy and treatment efficacy in colorectal cancer care, emphasizing the importance of a multidisciplinary approach in healthcare innovations.
[13]	2024	Application of Blockchain, IoT, and AI in Logistics and Transportation	Reviews how these technologies can enhance efficiency, transparency, and security in logistics operations, providing insights into their collaborative potential for optimizing supply chain management.
[4]	2023	Challenges and Solutions for Implementing AI, IoT, and Blockchain in Construction	Identifies key barriers to the adoption of these technologies in the construction sector and proposes strategic solutions to facilitate their integration, thereby enhancing project management and operational efficiency.
[14]	2024	Blockchain-Federated Learning for Enhancing IoT Security	Discusses the innovative approach of using federated learning combined with blockchain to bolster security measures in IoT systems, addressing vulnerabilities while ensuring data privacy and integrity.

AI, Artificial Intelligence; BCT, Blockchain Technology; IoT, Internet of things; ML, machine learning.

Unlike reviews focused solely on one sector such as logistics [13], construction [4], and colorectal cancer treatment [12], our research proposes integrated and standardized frameworks applicable to multiple industries. We identify specific challenges in scalability and data management, and propose solutions to overcome these obstacles.

Furthermore, we go beyond current reviews (e.g., [14]) by proposing policy recommendations and concrete solutions for scalability and security, integrating advanced cryptographic methods and data privacy frameworks. This approach ensures responsible and innovative development of IoT, blockchain, and AI technologies.

II.3 Our contributions

This survey is proposed based on existing relevant research to better understand the challenges and opportunities related to the integration of BCTs and AI in IoT systems.

Specific contributions to this study include:

We review related studies on the use of blockchain and AI in IoT. To highlight the improvements and enhancements achieved through the integration of these technologies, we divide the discussion into three principal areas: the integration of IoT with BCT, IoT with AI, AI with BCT, and the comprehensive integration of IoT with both blockchain and AI. This detailed examination allows us to understand the unique contributions and benefits of each type of integration.

The survey highlights the strengths and weaknesses of existing research on integrating IoT with blockchain and AI. Many crucial factors, such as decentralization, security, privacy, confidentiality, authentication, performance, and resilience, are examined. By analyzing these parameters, we aim to provide a balanced view of the advantages and disadvantages of the current approaches in order to identify areas that require further improvement.

Additionally, we identify various research challenges and future areas for designing effective IoT frameworks that integrate BCT and AI. This discussion aims to enable efficient IoT models with significantly improved application performance. We explore the obstacles, such as data complexity, scalability, and security, which need to be addressed, and suggest potential research directions to face these challenges and exploit the full potential of these technologies.

Key points of our study include a comprehensive review that synthesizes the current state of research

on blockchain, AI, and IoT integration, providing a valuable resource for researchers and practitioners. We systematically categorize different types of integrations and highlight their unique benefits and challenges. By analyzing critical factors such as security, scalability, and interoperability, we identify gaps in existing research and propose future directions. These points provide a clear overview of the current landscape and guide future research efforts.

Our contributions are multifaceted. First, we provide an in-depth analysis of the strengths and weaknesses of existing research, providing a balanced view of current approaches. Second, we identify key research challenges and suggest potential solutions to address them, paving the way for more effective IoT frameworks. Third, we highlight the importance of developing standardized protocols, scalable blockchain architectures, and advanced cryptographic methods to improve data security and privacy. Finally, we propose practical applications and policy-related recommendations to ensure the responsible development and deployment of these technologies. Our study serves as a basis for future explorations and offers insights that could lead to significant advances in the field.

The flowchart shown in Figure 4 summarizes and illustrates the contribution of this work by highlighting the key stages of the analysis, starting with a review of existing studies and culminating in the identification of challenges and future directions for research.

III Background

III.1 Blockchain basics

3.1.1 Overview of blockchain

BCT was initially introduced as a digital ledger for the cryptocurrency Bitcoin [15], but later it has evolved into a revolutionary concept with vast potential applications beyond finance. Its ability to securely store data, provide transparency, and create a decentralized network has opened many possibilities for innovation.

The evolution of BCT started with the creation of Bitcoin in 2009, where blockchain was used to record transactions on a public ledger [15]. Since then, BCT has evolved significantly, with new iterations improving upon the original design. The second generation of BCT technology, referred to as Ethereum, brought forth smart contracts [16]. These are self-executing agreements that automatically enforce the terms and conditions without requiring intermediaries.

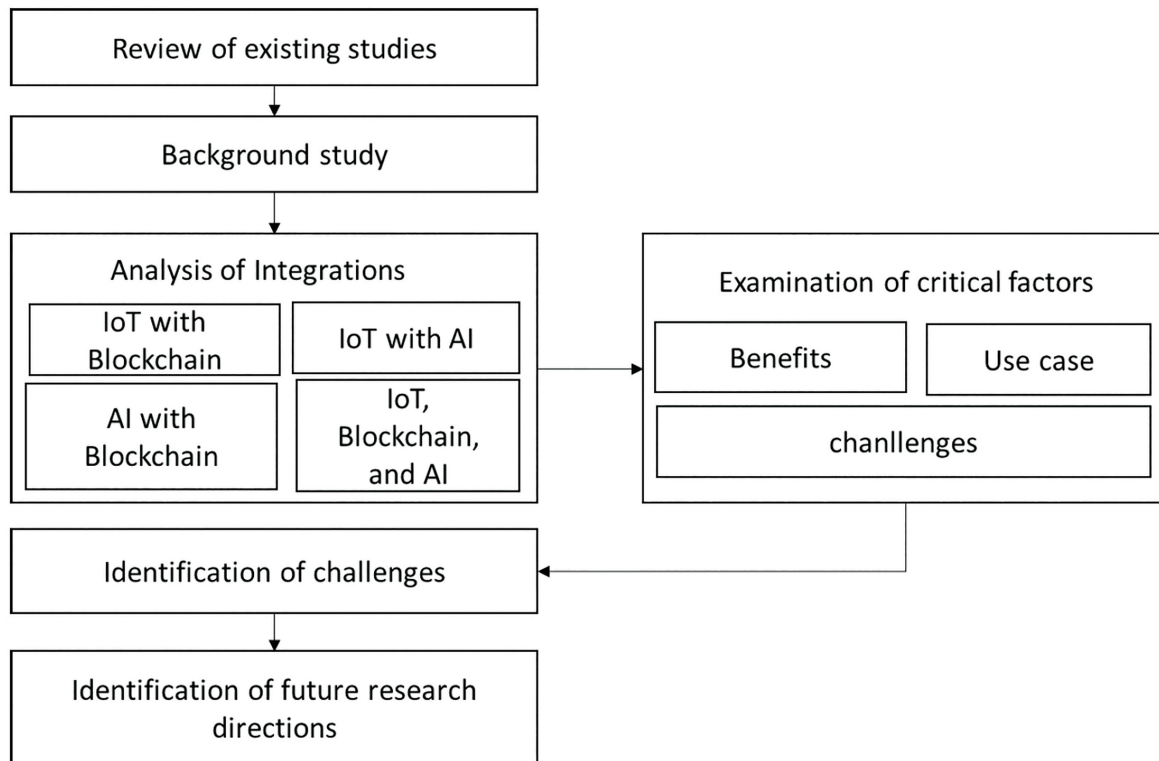


Figure 4: Flow diagram of the contributions. AI, Artificial Intelligence; IoT, Internet of things.

BCT leverages distributed consensus, immutability, and transparency to create a secure and reliable record of activities and decisions [2]. It offers tangible benefits in redefining established standards in security, transparency, and data management, making it a crucial component of decentralized systems [17]. The potential applications of BCT are vast and varied, ranging from finance to healthcare to supply chain management. For instance, BCT offers functionalities like data integrity, security, immutability, and verifiability, potentially improving the resistance to breaches of sensitive medical information [17].

Additionally, BCT offers the opportunity to establish a decentralized infrastructure that facilitates secure and direct connections between service providers and customers. This innovative approach eliminates the need for intermediaries, fundamentally transforming the way transactions and interactions occur. This decentralized framework not only minimizes transaction costs but also mitigates the risks associated with third-party involvement. Ultimately, the implementation of blockchain in this context fosters a more efficient, cost-effective, and trustworthy ecosystem for service transactions.

3.1.2 Components of blockchain

BCT operates on the principle of using blocks linked together in a chain through a cryptographic hash function. As illustrated in Figure 5, the structure of a block consists of various key components: a Node, which represents a computer within the blockchain framework and serves as the foundational element of the network; a Transaction, which is the smallest building unit of the blockchain, encompassing records and information that fulfill the blockchain's purpose; Blocks, which are information structures used to store a collection of transactions and are distributed across all nodes in the network, containing elements such as version number, previous hash value, timestamp, and Merkle root; a Chain, which refers to the sequence of blocks arranged in a specific order, forming the backbone of the blockchain; Miners, who are specialized nodes tasked with authenticating these blocks before they are appended to the blockchain structure, ensuring the integrity and security of the data; and Consensus, which is a set of protocols and standards that govern the execution of

blockchain operations, ensuring that all nodes in the network agree on the validity of transactions and the overall state of the blockchain. This interconnected system ensures the robustness, security, and reliability of BCT [18].

In a broader context, blockchain systems can be classified into three main types: public, private, and consortium, based on access control. Public blockchains are open to all for participation and data viewing [18]. Private blockchains restrict access to authorized members within an organization. Consortium blockchains, a hybrid approach, involve a pre-selected group governing a semi-decentralized network, offering controlled participation with some public blockchain benefits [18].

3.1.3 Features of blockchain and limitation

BCT offers several features that make it an attractive solution for various applications. These features include decentralization, security, transparency, and immutability [19]. Decentralization eliminates the need for intermediaries, allowing direct connections between service providers and customers. Security is enhanced, minimizing the risks associated with third-party involvement. Transparency is achieved by allowing all participants to access and verify the information on the network. The inherent immutability of BCT guarantees that data remain unaltered and undeletable after recording, which safeguards the integrity of the information.

While BCT offers significant potential benefits, it also faces several limitations and challenges (e.g., [20]). One major limitation is scalability, as the distributed nature of the blockchain can limit transaction throughput and processing speed. Blockchain

networks also have high energy consumption, particularly those using proof-of-work consensus mechanisms, which has raised concerns about their environmental impact. There are still regulatory uncertainties around blockchain and cryptocurrencies, creating challenges for adoption. Widespread adoption may be hindered by factors like technical complexity, user education, and integration with existing systems. Privacy is another concern; while blockchain provides a degree of anonymity, there are still risks of de-anonymization and misuse of transaction data. Researchers have identified incompatibilities between the characteristics of public blockchains and general traceability requirements in supply chains, limiting their usefulness. Overall, while blockchain is a promising technology, its limitations must be addressed in order to reach its full potential across industries.

While security is one of the main benefits of blockchain, it also poses major challenges as outlined in an earlier study [21]. These challenges include 51% attacks, forking issues, eclipse attacks, address attacks, and limited scalability.

In case of 51% attacks, a community of attackers takes control of more than 50% of the computing power of the network, allowing them to manipulate the transaction and transaction history to double spend. This raises the issue of trust in technology.

Forking problems are another major concern. A fork can occur accidentally due to discrepancies in block validation rules or intentionally during protocol updates, which can create divisions in the network. This can confuse users and undermine the unity of the system.

In addition, eclipse attacks illustrate another flaw in the security of decentralized networks. These attacks target specific users by isolating their nodes from the rest of the network, leaving them vulnerable to manipulation. Added to this are application bugs, which is

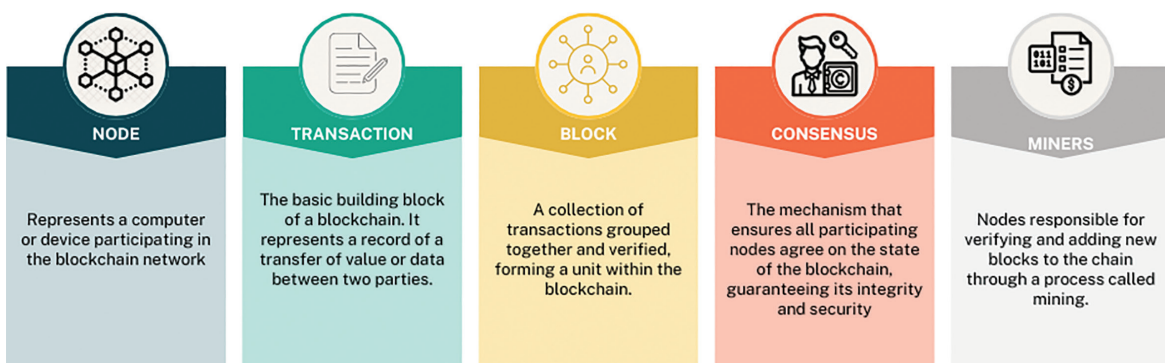


Figure 5: Blockchain components.

often the result of human error in code development. These flaws can create entry points for cyberattacks or functional failures.

Other challenges include shortened address attacks, where incomplete data allow an attacker to exploit weaknesses in the Ethereum Virtual Machine (EVM) to manipulate smart contracts. In addition, the dependency on timestamps represents a vulnerability that malicious miners can exploit by slightly altering transaction times to maximize their rewards or manipulate blocks.

Structurally, limited scalability remains a major challenge. Blockchain networks, particularly public networks such as Bitcoin and Ethereum, are often slow because of the consensus validation process, which can slow down their large-scale adoption, particularly in businesses. Complex regulatory constraints are also a major barrier. The lack of harmonized legislative frameworks and central bank policies makes it difficult to adopt blockchain in sensitive sectors such as finance or healthcare.

While blockchain offers unrivaled security, these challenges underline the need for technical and organizational solutions to ensure its effectiveness and resilience in the face of growing threats.

III.2 IoT basics

IoT is a network of physical devices, vehicles, structures, and other objects that are equipped with sensors, software, and communication capabilities to enable data gathering and sharing [22]. It has recently gained popularity because of its potential for advancement in important industries such as transportation, healthcare, and manufacturing. The key component of IoT is the smooth exchange of sensor data generated by IoT devices via connections to an IoT gateway. This gateway serves as a hub streamlining massive data transfer from several IoT devices [23]. This integrated infrastructure ensures quick and continuous data interchange and analysis, allowing businesses to increase operational efficiency, streamline decision-making processes, and stimulate innovation.

The data can also be sent to an edge device where it is analyzed locally, reducing the volume of data sent to the cloud and minimizing bandwidth consumption. Furthermore, IoT applications use ML algorithms to analyze vast amounts of data from sensors connected to the cloud, which results in real-time IoT dashboards and alerts that provide visibility into key performance indicators (KPIs), average time between failures, and other data. Even though IoT has many

benefits, it also has drawbacks such as cost, complexity, and evolution.

To optimize network bandwidth and minimize data storage in the cloud, some IoT applications can pre-process data at the edge. This involves sending data to local devices for initial analysis, reducing the amount of data sent to the cloud. Meanwhile, in the cloud, powerful ML algorithms can analyze massive datasets from connected sensors. This creates real-time dashboards and alerts with valuable information, including KPIs, mean time between failure (MTBF) statistics, etc. Despite its benefits, implementing IoT solutions comes with challenges such as cost, scalability, and system complexity.

3.2.1 Features of IoT system

IoT applications and services share certain common characteristics, each playing a crucial role in shaping the efficiency and effectiveness of IoT ecosystems:

- **Interoperability:** At the core of IoT functionality is the ability for devices and systems to communicate seamlessly with one another, irrespective of their underlying technologies or manufacturers. This interoperability fosters a cohesive and interconnected network, allowing disparate devices to collaborate and share data effortlessly. Whether it is a smart thermostat interacting with a home security camera or a fleet management system coordinating with vehicle sensors, interoperability ensures the smooth operation of IoT environments [24].
- **Scalability:** The dynamic nature of IoT demands systems that can adapt and grow with the expanding network of connected devices and the ever-increasing flow of data. Scalability in IoT architecture enables seamless expansion to accommodate new devices and handle the escalating volume of data generated by IoT networks. By employing scalable infrastructure and protocols, IoT deployments can efficiently manage resources, optimize performance, and support the evolving needs of businesses and consumers alike [24].
- **Security measures:** As the number of connected devices increases, the risk of security breaches and vulnerabilities also increases. Robust security measures are paramount to safeguard IoT devices, networks, and the sensitive data they manage. Multiple layers of security, including encryption, authentication mechanisms, secure firmware updates, and intrusion detection systems (IDS), are employed

to mitigate risks posed by unauthorized access, hacking attempts, and data breaches. By prioritizing security, IoT stakeholders can instill trust and confidence in their deployments, ensuring the integrity and confidentiality of data transmitted and processed within IoT ecosystems [25].

- **Data analytics capabilities:** The vast amounts of data generated by IoT devices present both challenges and opportunities. IoT applications leverage advanced data analytics techniques to collect, process, and derive actionable insights from diverse data sources. By harnessing the power of ML algorithms, predictive analytics, and real-time processing, IoT solutions can unlock valuable insights, optimize operations, and drive innovation across a myriad of sectors. From predictive maintenance in manufacturing plants to personalized healthcare interventions based on wearable device data, robust data analytics capabilities enable informed decision-making and drive tangible business outcomes in IoT deployments [26].
- **Dynamism:** Devices can be added, removed, connected, or disconnected from a network at any time, making IoT environments highly dynamic. Devices, software, and networks can become faulty or compromised, making device volatility very common in IoT environments [27].
- **Portability:** Certain devices have a high degree of mobility by design, such as cellphones and devices built into cars. This means that they may be subject to many administrative domains during their lifetime.

These common characteristics form the basis of successful IoT applications and services, enabling organizations to exploit the full potential of connected devices and data-driven information in the digital age. However, they also pose several security and privacy challenges, necessitating stringent IoT security requirements.

III.3 ML basics

ML is an important field of AI that enables machines to perform specific tasks using learning methods. Over time, ML models have demonstrated extraordinary skills, outperforming humans in a variety of disciplines by utilizing previous experiences to complete assigned tasks [28].

3.3.1 The ML approaches

ML algorithms are classified into several key categories, each representing a distinct approach to learning. Figure 6, a visual representation of these paradigms, illustrates their core principles and relationships:

Supervised learning is a widely used ML paradigm where the algorithm is provided with labeled training data, and it learns to predict the output for new inputs [29]. Supervised learning techniques include classification (predicting discrete labels) and regression (predicting continuous values). Some common supervised learning algorithms support SVMs [30].

Semi-supervised learning bridges the gap between supervised and unsupervised learning by

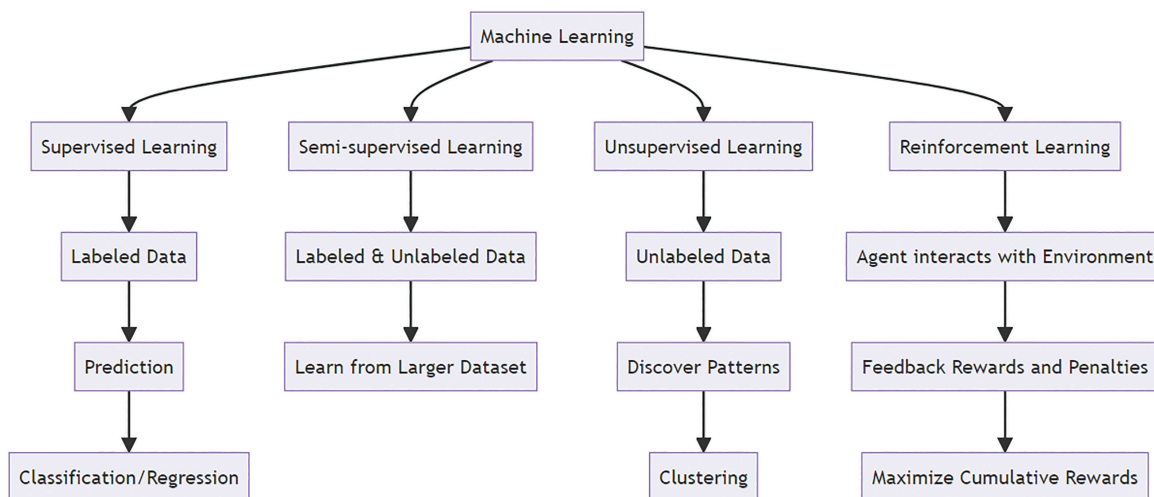


Figure 6: ML algorithms. ML, machine learning.

exploiting both labeled and unlabeled data. This approach is particularly useful when labeled data is scarce or expensive to acquire, as it allows models to learn from a larger amount of information while benefiting from the guidance of labeled examples.

Unsupervised learning involves discovering hidden patterns and structures in unlabeled data, often through methods like clustering. This is in contrast to the labeled data used in supervised learning [29].

Reinforcement learning is a learning paradigm where an algorithm learns by interacting with a dynamic environment and receiving feedback in the form of rewards or penalties. The goal is to learn an optimal sequence of actions to maximize the cumulative reward [31].

3.3.2 ML processes

Generally, building a new ML model generally consists of two main stages: training and testing, which are required for tasks such as prediction, classification, and clustering on fresh datasets (Figure 7). Data are emerging as a significant asset in ML, playing a key role in both preprocessing and training models. Initially, the ML model is trained on a specific dataset, with the effectiveness of the ML classifier increasing as the training data size grows. Following training, the model's prediction accuracy is evaluated using a new dataset, leading to deployment if accuracy fulfills the criteria; otherwise, more training is performed. Recent improvements have seen DL emerge as a significant ML subgroup aiming to mimic human cognitive processes. Rooted in cognitive theories, DL structures are inspired by neural networks, with applications ranging from object identification to facial recognition and traffic flow prediction, demonstrating the range of its influence.

ML algorithms have proven useful in a variety of industries, including transportation, image processing, and the banking sector [32]. A broad range of models exist in the field of ML to handle various issue types, with SVM, artificial neural networks (ANN), and decision trees among the most commonly used [33].

IV Blockchain in IoT framework applications

The growth of IoT presents a complex set of challenges in many areas. These challenges encompass issues such as resource constraints, central server overload, and the potential worry of unauthorized data access. Addressing these challenges requires a multifaceted approach that involves optimizing resource utilization, improving server scalability, and implementing robust security measures to protect sensitive data. By proactively addressing these challenges, the full potential of IoT technologies can be realized, while ensuring the integrity, confidentiality, and efficiency of IoT systems across a wide range of applications and industries.

BCT is an innovative solution that offers significant advantages in meeting these challenges. Blockchain provides a decentralized system where peer-to-peer (P2P) consensus can be achieved without the need for a central authority, mitigating the risks associated with overloading central servers and unauthorized access. Thanks to P2P communication facilitated by blockchain, IoT devices can interact securely, exchange data, and verify transactions, improving the overall efficiency and reliability of IoT networks. In addition, the transparency and immutability inherent in blockchain reinforce trust between stakeholders without relying on a trusted third party, addressing concerns about data integrity and confidentiality. In addition, smart contracts, a feature of BCT, enable transactions to be controlled by predefined conditions and functions, providing a mechanism for enforcing agreements and automating processes within IoT ecosystems. By leveraging the blockchain's consensus mechanism, P2P communications, trust-building capabilities, and smart contract functionality, IoT systems can effectively overcome the challenges posed by resource constraints, server overload, and security threats, ensuring the seamless operation and reliability of IoT applications in a wide range of sectors.

When comparing the flow of information between IoT and blockchain technologies, several key differences emerge. In terms of confidentiality, IoT systems



Figure 7: Building ML model steps. ML, machine learning.

often face a lack of privacy due to centralized data storage, whereas blockchain guarantees the confidentiality of participating nodes through decentralized consensus mechanisms. Bandwidth usage varies, with IoT devices constrained by limited bandwidth and resources, while blockchain transactions generally require higher bandwidth consumption. System structure also diverges, with IoT tending to be centralized, while blockchain operates on a decentralized network. Scalability is an issue for IoT networks, especially with a large number of devices, while blockchain's scalability is limited, especially with extended networks. Resource allocation differs, with IoT being resource-constrained and blockchain being resource-intensive. Latency requirements are low for IoT, but blockchain faces time-consuming block extraction processes. Finally, security issues are common in IoT, whereas blockchain offers better security measures thanks to its decentralized and immutable nature.

Table 3 illustrates the comparison between IoT and blockchain discussed earlier.

The combination of IoT and BCT has the potential to revolutionize various application domains, including intelligent traffic systems, e-commerce, and smart cities, as described in Table 4, which we will elaborate on with specific examples.

In the context of intelligent traffic systems [36], blockchain can facilitate decentralized communication between vehicles, eliminating the need for a central computing node and enhancing energy efficiency. By integrating blockchain with IoT-based smart city applications, cybersecurity issues can be addressed, and a sustainable smart city vision can be achieved.

For instance, in the e-commerce domain, NormaChain has been proposed to manage IoT-based transactions [35]. This system aims to ensure

autonomy, lightness, and legitimacy in transaction management, eliminating the dependence on a central authority and achieving fully decentralized governance.

In the smart city ecosystem, BCT can enhance and optimize IoT-based intelligent traffic systems by allowing vehicles to collaborate without relying on a central computing node. This decentralized approach can lead to energy savings, reduced network throughput, and the potential for expansion to introduce new monitoring and execution processes in the existing blockchain-based system.

Moreover, blockchain can improve the protection of personal data collected in smart cities, making it easier for solar-powered households to trade surplus electricity automatically. It can also facilitate direct communication between government departments and the public, enhancing accountability and ensuring data integrity.

In summary, the integration of blockchain and IoT technologies offers significant potential for various application domains, including intelligent traffic systems, e-commerce, and smart cities. By addressing cybersecurity concerns, enabling decentralized communication, and enhancing data protection, this combination can lead to more efficient, secure, and sustainable systems.

V IoT and AI Applications

AI and IoT integration has the potential to revolutionize various industries, improving efficiency, decision-making, security, and personalization. This symbiotic relationship between AI and IoT can address challenges, including data management privacy, connectivity, energy usage, and cost-effectiveness. The vast volume of data generated by IoT devices can be managed and processed efficiently by AI

Table 3: Comparison between IoT and BCT

Items	IoT	Blockchain
Privacy	Lack of privacy	Ensures the privacy of the participating nodes
Bandwidth	IoT devices have limited bandwidth and resources	High bandwidth consumption
System Structure	Centralized	Decentralized
Scalability	IoT contains a large number of devices	Scales poorly with a large network
Resources	Resource restricted	Resource consuming
Latency	Demands low latency	Block mining is time-consuming
Security	Security is an issue	Has better security

BCT, blockchain technology; IoT, Internet of Thin

Table 4: Studies combining IoT and BCT

Reference	Contribution	Strength	Weakness	Application domain
[34]	Proposes a novel framework with a new on-demand market model, namely, DCDM follows a P2P model, differentiated from conventional IDM models by integrating operational factors.	- The ability of the framework to exchange not only datasets but also the skills of data providers, using integrated operational factors. - Use of a revolutionary approach combining blockchain and crowdsensing to demonstrate relevance in the IoT context.	- Lack of scalability when faced with a large number of IoT data streams. - Need for a robust solution to manage high volumes and speeds of IoT data. - System performance is subject to degradation as the number of IoT devices increases.	Marketplace
[35]	Proposes a three-layered sharding blockchain network model-based autonomous transaction settlement system specifically designed for IoT e-commerce.	Integrates the blockchain solution specifically designed for IoT e-commerce to meet challenges such as autonomy, lightness, and legitimacy of the transaction management system and to eliminate dependence on a central authority, achieving fully decentralized governance that equitably distributes supervisory power.	Insufficient detailed exploration is evident regarding how NormaChain precisely tackles the complexities associated with handling extensive data, encompassing aspects such as managing transaction volumes, ensuring data integrity, and minimizing latency within an IoT framework.	E-commerce
[36]	Introduces blockchain as a decentralized technology to allow vehicles jointly collaborate without having to go through a central computing node authority in IoT-based Intelligent Traffic Systems.	Focuses on data transmission and request for lane property right under the domain of an intelligent traffic system.	- Power energy consumption - Huge overload of network throughput - Expandability to introduce new monitor and execution processes in the existing blockchain-based system.	Smart city
[37]	Proposes a PKI system based on BCT to store and verify the digital certificate in a decentralized way.	Uses blockchain in verifying certificates efficiently without the participation of a third party. Improves the scalability and security of the IoT applications by using the distributed characteristics of the chain.	- Lack of a detailed examination of potential challenges related to data processing. - Insufficient exploration of how the proposed PKI manages the volume and speed, and efficiency of data processing would contribute to a more comprehensive understanding of the practical implications and potential limitations of the proposed solution.	PKI

(Continued)

Table 4: Continued

Reference	Contribution	Strength	Weakness	Application domain
[38]	- Examines various proposed frameworks in the literature, focusing on their use of BCT to enhance IoT forensics. - Evaluates the readiness of blockchain integration in addressing challenges.	- Addresses the challenges associated with data integrity, shared storage, identification, transparency, and privacy in IoT forensics. - Addresses factors when integrating BCT into IoT forensics.	Data processing	Forensics
[39]	- Proposes a new protocol called blockchain-based IoMT. - Authenticated Key Exchange BloMTAKE establishes a private/consortium blockchain-based distributed protocol that eliminates the need for a single trusted authority and ensures secure access to data generated by IoMT devices.	- Merges blockchain and IoT in one system to lead to issues such as higher latency, centralization, and a single point of failure. Improves secure access to data generated by IoMT devices by establishing a secured shared session for authenticated devices to prevent unauthorized - access.	- Lacks an in-depth exploration of its scalability, especially concerning the potential surge in data volume as the IoT devices generate a large amount of heterogeneous data that do not delve into potential data transmission latency issues that may arise in a blockchain-based distributed environment.	Healthcare
[40]	- Establishes a comprehensive IoT forensic process integrated with BCT to enhance digital evidence preservation, addressing authenticity, integrity, confidentiality, and privacy concerns in the IoT ecosystem, ultimately demonstrating a high-throughput, low-latency, and error-free blockchain-enabled platform through rigorous evaluation in a simulated smart home environment.	- Explores the blockchain technologies' ability to address challenges, such as digital evidence authenticity, integrity, confidentiality, and privacy, which may impact the investigation process in IoT forensics. - Proposes a holistic forensic process and identifies blockchain integration patterns to establish a secure and scalable architecture.	- Lack of improvement in the quality of evidence, particularly IDS alerts, which can be addressed through the application of ML techniques or algorithms.	Smart home

(Continued)

Table 4: Continued

Reference	Contribution	Strength	Weakness	Application domain
[41]	Improves the stability and efficiency of IoMT, strengthens the security and privacy of personal information, and creates a healthy and safe network environment by combining basic blockchain knowledge with the Fuzzy Sets Theory.	- Development of a hybrid IDS using blockchain and Fuzzy Sets Theory, demonstrating exceptional accuracy in identifying various behaviors within the IoT for maintaining data security and IoMT functionality. - Explores the security problems related to user privacy data based on blockchain and Fuzzy Sets Theory.	- Does not apply the method to mobile sensing nodes. - Absence of real-world validation or deployment of the proposed hybrid intrusion detection method.	- IoMTs
[42]	Provides a complete analysis of the enablers for using blockchain IoT to manage logistics and supply chains.	- The use of the technology–organization–environment theories to examine blockchain–IoT adoption enablers. - A framework based on the Graph Theory Matrix Method to measure the extent of a readiness to adopt blockchain IoT.	- Complex evaluation process. - Limited expert involvement - Lack of technical performance - Analysis suggests the need for further research to conduct a comprehensive cost analysis of the technical infrastructure and evaluate the technical performance of BloT in terms of scalability, throughput, storage, and latency on a network.	- Logistics and Supply Chains Management - Industry 4.0

BCT, blockchain technology; BloMTAKE, Blockchain-based IoMT authenticated key exchange; DCDM, decentralized IoT collectability data marketplace; IDM, IoT data marketplace; IDS, intrusion detection systems; IoMT, Internet of medical things; IoT, Internet of things; ML, machine learning; NormaChain, Blockchain-based normalized autonomous transaction settlement system; P2P, peer-to-peer; PKI, public key infrastructure.

algorithms, enabling smarter decisions and real-time actions. However, it is crucial to process and preserve these data so that AI systems can access them easily. Another important issue is security, as IoT devices in many cases are installed in unprotected spaces, exposing them to cyberattacks. To guarantee data and system integrity, strict security measures need to be implemented. Integrating AI algorithms into IoT devices can be difficult, as companies often use different protocols and standards for their development. Successful AI integration requires the development of standardized norms and protocols for IoT devices. As IoT devices often run on batteries, energy efficiency is a key element in their conception algorithms have the potential to be very demanding in terms of computation and energy consumption. Therefore, one of the key factors in integrating AI into IoT is the creation of low-power AI algorithms. Implementing AI in IoT can be prohibitively expensive, particularly for small- and medium-sized enterprises. It is therefore essential to find affordable ways to properly combine AI and IoT.

With the help of AI, large amounts of data generated by IoT devices can be processed, leading to both making more intelligent decisions and taking actions in real time. AI algorithms can discern patterns, correlations, and anomalies in data, providing valuable insights and enabling informed decisions, predictions, and automated responses. ML algorithms, a subset of AI, are often used in IoT systems as part of the data processing stage. Different ML paradigms, such as supervised learning, unsupervised learning, and reinforcement learning, can be used to discern patterns, correlations, and anomalies in the data. For example, in a smart home scenario, ML can predict user preferences based on historical usage patterns, adjusting lighting, temperature, or security settings accordingly. Anomaly detection algorithms can identify irregularities in sensor data, alerting users to potential problems or security threats.

The combination of AI and IoT offers many benefits, including increased automation, predictive insights, and adaptability. These benefits can optimize operations, improve resource efficiency, and enhance user experiences in a variety of industries or domains. However, challenges can arise, such as managing and storing substantial amounts of data, ensuring security, solving interoperability issues, optimizing energy consumption, and controlling costs. As a result, organizations can apply AI to enhance the effectiveness and overall performance of IoT devices by addressing these obstacles.

Table 5 provides an overview of several works in the fields of AI and IoT, and their applications across

different domains, showcasing their objectives, methodologies, key findings, strengths, weaknesses, and application domains.

V.1 Challenges of ML and DL integration with IoT

The integration of ML and DL techniques with IoT is a promising direction to address the security challenges posed by the scale, heterogeneity, and real-time nature of IoT networks. Continued research in this area is crucial to develop robust, scalable, and privacy-preserving security solutions for the IoT ecosystem. Table 6 outlines several studies that focus on these aspects, providing insights into their challenges and proposed solutions.

VI Blockchain and AI

VI.1 Benefits of combining blockchain with AI

The combination of BCT and AI presents a powerful synergy that offers numerous benefits across various industries. Blockchain's decentralized and immutable ledger provides a secure environment for storing and sharing data, which is crucial for AI systems that require vast amounts of reliable data to function effectively. This integration ensures data integrity, preventing tampering and unauthorized access, while also allowing for verifiable and traceable AI decision-making processes, fostering trust among stakeholders. Furthermore, blockchain can facilitate the sharing of high-quality, verified data across different entities, which can then be used by AI algorithms to generate more accurate and insightful predictions, particularly valuable in the fields like healthcare. The integration of blockchain and AI can also enable decentralized AI models, where multiple parties can contribute to and benefit from AI advancements without the need for a central authority, promoting innovation and collaboration. Finally, the combination of these technologies can enhance automation and efficiency in various processes, such as using smart contracts powered by blockchain to automate transactions and agreements based on AI-generated conditions and insights, reducing the need for intermediaries and accelerating operations across diverse applications.

VI.2 Blockchain and AI use case

The use of combined BCT and AI has proven their efficiency in several domains by improving

Table 5: List of works in AI and IoT fields

Reference	Objective	Methodology	Key findings	Strengths	Weaknesses	Application domain
[43]	Presents the smart city concept, background of smart city development, and components of the IoT-based smart city. Conducts a literature review on recent IoT-enabled smart city developments and breakthroughs empowered by AI.	Literature review on smart cities, IoT, and AI. Analysis of recent developments, trends, and challenges.	Highlights the current stage, major trends, and unresolved challenges of adopting IoT and AI technologies for smart cities.	Comprehensive analysis of current trends and challenges. Clear recommendations for future research.	May lack in-depth analysis of specific case studies or regional differences.	General smart city applications, including transportation, healthcare, and agriculture.
[44]	Introduces a hybrid topology for IoT applications integrating mesh and star wireless sensor configurations to optimize energy consumption and ensure comprehensive network coverage.	Empirical data analysis from 380 sensors in Vitória connected to a central gateway in Vila Velha. Utilization of k-Medoids algorithm for mesh network clustering and GA for star network points determination.	Empirical data analysis from 380 sensors in Vitória connected to a central gateway in Vila Velha. Utilization of k-Medoids algorithm for mesh network clustering and GA for star network points determination.	Demonstrates the effectiveness of planning and resource allocation algorithms in reducing the number of mesh networks and allocating resources efficiently.	Innovative hybrid topology, combining mesh and star configurations. Efficient use of algorithms for clustering and resource allocation.	Specific to the geographical context of Espírito Santo, Brazil; may need adaptation for other regions.
[45]	Designs a global model using IoT and AI to control residential energy consumption and reduce carbon emissions.	A model trained using the DT algorithm. Unique data sequences are created for each unit, with data minimization and central intelligence direction.	Model pre-simulation shows a 21% reduction in annual carbon emissions by controlling connected devices.	Effective use of AI and IoT for practical carbon emission reduction. Demonstrates significant potential impact.	Needs further development and medium-term implementation. Global applicability is yet to be fully tested.	Energy consumption control in residences to combat global warming.

(Continued)

Table 5: Continued

Reference	Objective	Methodology	Key findings	Strengths	Weaknesses	Application domain
[46]	Proposes the EO-LWAMCNet model to predict chronic health conditions (kidney or heart disease) using IoT data.	Sensors collect patient data, which are transmitted to the cloud. The EO-LWAMCNet model classifies the data using CKD and HD datasets. Performance was evaluated with accuracy, MCC, F1-score, and miss rate.	Achieves 93.5% accuracy with the CKD dataset and 94% accuracy with the HD dataset. Low miss rate in classification.	High accuracy and low miss rate in predicting chronic diseases. Utilizes IoT and AI effectively for healthcare.	May require further validation with larger and more diverse datasets.	Healthcare, particularly in predicting and managing chronic diseases like heart and kidney diseases.

AI, Artificial Intelligence; CKD, chronic kidney disease; DT, Decision Tree; GA, genetic algorithm; HD, Heart Disease dataset; IoT, Internet of things; LWAMCNet, Lightweight Automatic Modulation Classification Network; MCC, Matthews Correlation Coefficient.

security, efficiency, and transparency. This synergy is particularly impactful in domains like healthcare, where it enhances data management and transaction authentication, ensuring the integrity of patient records. In transportation, the integration of BCT and AI boosts operational trustworthiness and efficiency, providing innovative solutions to persistent challenges. These advancements demonstrate the significant potential of BCT and AI to address critical issues and elevate performance across various sectors described in Table 7:

VI.3 Blockchain and AI challenges

The integration of blockchain and AI has the potential to revolutionize various industries by enhancing security, efficiency, and transparency. However, this integration is not without its challenges that must be addressed to ensure seamless operation. Primary challenges are given as follows.

• Data complexity and interoperability

Data complexity and interoperability are two major challenges in integrating blockchain and AI. BCT is based on decentralized and distributed data storage, which makes it difficult to integrate with AI systems that require structured and standardized data. This is because blockchain uses distributed data storage, which can make it difficult to access and manipulate data for AI systems that require organized and standardized data.

According to research detailed in a comprehensive review of the confluence of AI and blockchain technologies [54], the lack of interoperability between different blockchain platforms and AI systems can significantly hinder the smooth exchange of data. This review [54] has highlighted that the synergistic combination of these technologies, while beneficial in improving the performance and efficiency of existing information and communication technology (ICT) systems, is still in its infancy and subject to ongoing exploration.

Furthermore, the effectiveness of ML models depends on both the volume and quality of the data. According to a previous research [55], AI-based solutions to blockchain-related problems are often faced with limited or unreliable datasets. The lack of reference datasets that are free from mislabeling and have high diversity is evident.

The main data challenges in integrating blockchain and AI are as follows:

Table 6: Challenges addressed by ML and IoT

Reference	Challenge	Solution
[47]	Heterogeneity of IoT devices	Federated learning approaches enable collaborative learning while preserving privacy
[41,42]	Need for real-time data processing for security	Combining edge computing with deep learning to enable efficient security analytics close to the data sources
[47]	Scalability and confidentiality issues	Federated learning approaches enable collaborative learning across IoT devices while preserving privacy
[48]	Edge device limitations for ML/DL models	Hardware-assisted ML techniques to enable efficient ML on resource-constrained edge devices
[41,43]	Improves IoT security and optimization	Applying supervised learning for authentication, attack detection, and malware analysis using algorithms like SVM, KNN, and neural networks
[47]	Enhances IoT security and optimization	Using unsupervised learning for anomaly and intrusion detection with techniques like clustering (e.g., k-means) and density estimation
[47]	Adaptive security policies for DDoS attacks	Reinforcement learning approaches
[48]	Generates synthetic data for ML-based security	GANs

DDoS, Distributed Denial of Service; KNN, K-Nearest Neighbors; GANs, Generative adversarial networks; IoT, Internet of things; ML, machine learning.

Table 7: BCT and AI use cases

Item	Contribution	Strength	Weakness	Application domain
[50]	Gives an overview of how combining blockchain and ML technology can help in healthcare sectors.	- Checks whether the user initiating or requesting a transaction is a legitimate user. - Ensures that the user has the right to request the large characters of the transaction they are carrying out.	- Ledgers are only appendices. The transaction cannot be modified once it has been recorded. Details will be manually entered and human error will always be possible. Care should be taken or additional privileges should be granted to an authority. - BCT keeps a record of each transaction, including a copy of the history. The size of the database would increase, which could make it more complex to manage in the future.	Healthcare

(Continued)

Table 7: Continued

Item	Contribution	Strength	Weakness	Application domain
[51]	Explores the synergy between blockchain and AI Examines their applications in various industries, particularly in transportation.	- Blockchain and AI technology convergence with significant advantages in the transportation industry. - Blockchain could enhance AI applications in terms of trustworthiness, decentralized computing, effectiveness, transparency, and lower entry market barriers. - The AI applications could improve the blockchain in several aspects, including energy consumption, scalability, security, privacy, efficiency, hardware, and data gates.	- Storage capacity and scalability - Security and privacy - Limited data access - Domain identification	Transportation systems
[52]	- Enhances blockchain security with AI - Automates processes and reduces intermediaries - Analyzes data for insights	- Improves security, automation, transparency, efficiency, and predictive maintenance	- Energy consumption associated with blockchain. - Potential vulnerabilities - Data privacy concerns - Scalability	Industry 4.0
[53]	- Detects and prevents food safety hazards. - Maintains track of perishable food with an immutable ledger. - Streamlines supply chain, connecting farmers directly with customers. - Enhances efficiency, transparency, and sustainability in the food chain.	- Rapid and precise contamination detection. - Increased trust in the food supply chain. - Detailed bibliometric analysis and visualization.	- Reliance on a single bibliometric tool limits analysis depth. - Limited applications in other smart agriculture areas. - Potential data privacy issues. - Limitations in data collection methods.	Food safety, smart agriculture, supply chain management

AI, Artificial Intelligence; BCT, blockchain technology; ML, machine learning.

- The complexity of data on blockchain, which is often unstructured and distributed, makes it difficult for AI systems to use.
- The lack of interoperability between different blockchain platforms and AI systems hinders the smooth exchange of data.
- The limited volume and quality of datasets are available to effectively train AI models, in particular the lack of high-quality reference datasets.

- **Scalability and replicability**

Another significant challenge is the scalability and performance of blockchain and AI systems. AI systems require substantial amounts of data to function effectively, making the scalability of blockchain platforms a critical issue. The current limitations of BCT in terms of transaction processing capacity and data storage can hinder the efficient integration of AI systems, leading to delays and inefficiencies. This problem has also been highlighted in several studies. One such study [55] details why scalability is considered a major issue in systems that combine blockchain and AI. According to the study, the limited transaction throughput and the high latency of current blockchain platforms can significantly impair the performance of AI applications that rely on real-time data processing. Additionally, the immense data storage requirements of AI models can overwhelm blockchain networks, causing further performance bottlenecks and reducing overall system efficiency.

Regarding reproducibility in ML, which is crucial for the credibility of results, a major challenge arises when applying it to blockchain. Ensuring consistent results is crucial to developing reliable AI-enhanced blockchain systems [55]. However, several factors hinder this achievement, including the scarcity of standardized datasets, rapid advances in AI and blockchain, and complex interactions between algorithms and blockchain structures. The lack of reproducibility can hinder the adoption of AI-based solutions in blockchain, making resolving this issue indispensable for the successful integration of AI and blockchain technologies.

- **Security and privacy**

One of the most important challenges in merging BCT and AI technologies lies in ensuring security and privacy [56]. This integration introduces complexities that necessitate careful attention to safeguarding sensitive data and preventing unauthorized access.

According to a detailed examination of AI and blockchain convergence, the amalgamation of these technologies brings forth intricate security implications that demand thorough consideration.

AI systems rely heavily on extensive datasets for effective operation [56]. However, this reliance also amplifies the risks associated with data breaches and unauthorized access. The fusion of AI and blockchain exacerbates these concerns, as blockchain networks serve as repositories for sensitive transactional data that may become targets for malicious entities. This interconnectedness expands the potential attack surface, heightening the risk of data compromise.

Furthermore, leveraging AI within blockchain ecosystems introduces novel vulnerabilities [57]. Sophisticated AI algorithms can be exploited to launch intricate attacks on blockchain networks, utilizing their analytical capabilities to pinpoint and exploit system weaknesses. These AI-driven threats may target consensus mechanisms, manipulate transactional data, or circumvent security protocols, posing substantial risks to the integrity and stability of blockchain networks.

- **Explainability and transparency**

The integration of blockchain and AI also raises concerns about explainability and transparency. AI systems are often opaque and difficult to understand, which can make it challenging to identify and address biases and errors. The use of BCT can provide some transparency, but it is essential to ensure that the AI systems used in conjunction with blockchain are transparent and explainable.

- **Regulatory frameworks**

The integration of blockchain and AI also requires a clear regulatory framework. As AI systems are increasingly used in various industries, there is a need for regulatory bodies to develop guidelines and regulations that address the unique challenges and risks associated with AI-powered blockchain systems. In conclusion, the integration of blockchain and AI is a complex and challenging task. Addressing the data complexity, scalability, security, explainability, and regulatory challenges will be crucial to ensuring a seamless integration of these technologies. By understanding these challenges, we can work toward developing more efficient, secure, and transparent AI-powered blockchain systems that can revolutionize various industries.

VII Blockchain and AI with IoT architecture applications

VII.1 Benefits of combining blockchain, IoT, and AI

Several studies have examined the combination of blockchain, IoT, and AI technologies and identified a range of transformative benefits [5, 58, 59]. This combination offers disruptive benefits such as increased security, efficiency, and intelligence in data management systems. A detailed overview of key benefits is listed in Table 8:

- **Enhanced data security**

The rapid adoption of IoT comes with inherent security risks, particularly due to the limited processing power and vulnerability of connected devices. BCT offers a promising solution by leveraging its decentralized and immutable ledger, which ensures the integrity of data generated by IoT devices [9]. This inherent security feature safeguards against unauthorized access and tampering, allowing AI algorithms to safely analyze sensitive data without compromising privacy [9]. This enhanced data security is crucial for building trust in IoT ecosystems, allowing for the safe and secure deployment of these technologies in diverse applications. As highlighted in Table 9, blockchain excels in securing data by offering features like data encryption, hashing, authentication, and integrity, which are often limited or absent in traditional IoT and AI systems.

- **Improved decision-making**

The convergence of AI and BCT revolutionizes decision-making within IoT. Blockchain's immutable ledger ensures data integrity and authenticity, providing a foundation of trust for AI algorithms. This enables AI to generate more reliable insights from real-time data streams, facilitating predictive analytics, anomaly detection, and personalized recommendations [60]. For instance, in smart transportation, AI can analyze traffic patterns, weather data, and vehicle sensor readings to optimize traffic flow and improve safety. Blockchain can ensure the integrity of these data sources, making the AI's insights more trustworthy and actionable, leading to better decision-making. This synergy enhances trust in IoT systems by guaranteeing data security, transparency, and accountability, leading to more informed, efficient, and trustworthy actions across diverse IoT applications.

- **Increased efficiency**

The automation capabilities of AI, when fueled by real-time data from IoT devices and secured by blockchain, significantly enhance operational efficiency. AI can automate routine tasks, predict maintenance needs, and optimize processes, reducing manual intervention and accelerating response times. Blockchain ensures that the data driving these automations is accurate and tamper-proof [60]. For example, in a manufacturing setting, AI could analyze sensor data from machines to predict potential failures, allowing

Table 8: Key benefits of integrating BCT, IoT, and AI

Benefit	Description	Technologies involved		
		Blockchain	IoT	AI
Enhanced data security	Blockchain ensures data integrity and security, while AI analyzes it without compromising privacy.	✓		✓
Improved decision-making	AI processes real-time IoT data accurately, aided by the trustworthiness provided by blockchain.	✓	✓	✓
Increased efficiency	AI-driven automation with IoT data, secured and verified by blockchain.	✓	✓	✓
Traceability	Blockchain's immutable records ensure full traceability of IoT data and AI-optimized processes.	✓	✓	✓
Cost reduction	Optimization of processes through AI and IoT, with reduced intermediary costs via blockchain.	✓	✓	✓

AI, Artificial Intelligence; BCT, blockchain technology; IoT, Internet of things.

Table 9: Comparison of data security features

Feature	Blockchain	IoT	AI	Blockchain + IoT + AI
Data encryption	✓	Limited	✓	✓
Data hashing	✓	X	X	✓
Data authentication	✓	Limited	X	✓
Data confidentiality	✓	Limited	✓	✓
Data integrity	✓	Limited	X	✓

AI, Artificial Intelligence; IoT, Internet of things.

for proactive maintenance and minimizing downtime. Blockchain could then provide an immutable record of these predictions and maintenance actions, ensuring transparency and accountability in the process. This combination of AI and blockchain empowers organizations to streamline operations, optimize resource allocation, and improve overall productivity within their IoT ecosystems.

• Traceability

The convergence of blockchain, IoT, and AI creates a powerful ecosystem that ensures unparalleled traceability within complex systems, transforming industries where data integrity and transparency are critical. By seamlessly integrating these technologies, we gain the ability to track the origin, movement, and transformation of data across IoT networks with unprecedented accuracy and reliability [7].

In supply chain management [7], sensors embedded within goods constantly transmit data about their location, condition, and handling to a blockchain-based platform. AI algorithms can then analyze these data in real time, identifying potential risks or anomalies and triggering preventative actions. Blockchain ensures that every data point is immutably recorded, creating a transparent and auditable trail that can be accessed by all stakeholders. This eliminates the possibility of tampering or manipulation, fostering trust and accountability within the supply chain.

Similarly, in healthcare [7], this convergence can revolutionize patient data management. Sensors embedded within medical devices can constantly transmit patient vitals and medical information to a secure blockchain platform. AI algorithms can analyze these data, identifying potential health risks and suggesting personalized treatment plans. Blockchain guarantees the immutability and security of these

data, enabling secure and transparent data sharing between healthcare providers while safeguarding patient privacy.

This powerful combination of blockchain, IoT, and AI not only ensures traceability but also empowers stakeholders with actionable insights, enabling them to make more informed and efficient decisions. This transformative approach promises to reshape diverse industries, from supply chain management to healthcare, fostering greater trust, transparency, and innovation within the IoT ecosystem.

• Cost reduction

The combined use of AI, IoT, and blockchain can lead to significant cost reductions. AI and IoT optimize operational processes, reducing waste and inefficiencies. Blockchain reduces the need for intermediaries by providing a secure and transparent system for transactions and data exchanges. Together, these technologies lower operational costs and enhance the overall efficiency of business processes [7].

We can also streamline this combination as shown in Figure 8.

- **IoT data generation:** The IoT devices are the data sources, which constantly collect information from the real world (e.g., sensors monitoring energy usage, weather conditions, or even traffic patterns).
- **Blockchain data security and integrity:** Blockchain acts as a secure and tamper-proof ledger for the data generated by the IoT devices. It ensures that the data are trustworthy, accurate, and protected from manipulation.
- **AI data analysis and decision:** AI algorithms analyze the secure and reliable data stored on the blockchain. This analysis can lead to valuable insights and predictions, allowing for informed decision-making.

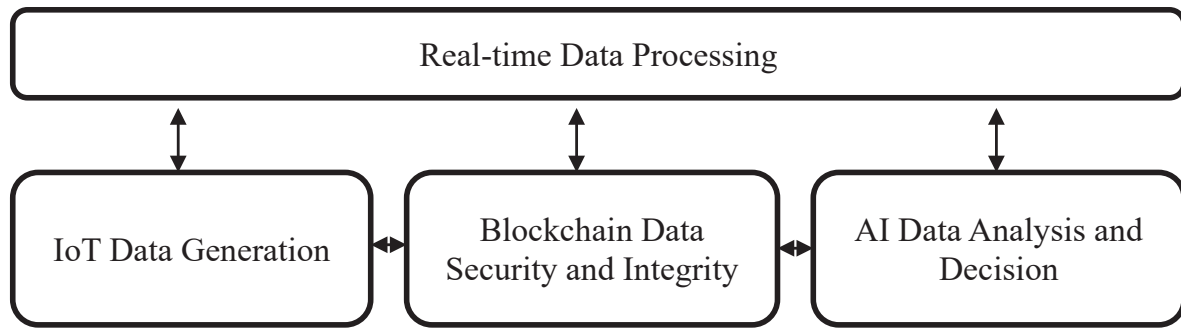


Figure 8: Combination of IoT, BC, and AI processes. AI, Artificial Intelligence; IoT, Internet of things.

Table 10: Applications of BCT, IoT, and AI convergence

Industry	Application	Key benefits
Supply chain management	Traceability and counterfeiting	Enhances security, transparency, and trust
Healthcare	Secure data sharing and privacy	Secures data management, privacy protection, and efficient access
Smart cities	Resource management and optimization	Improves efficiency, sustainability, and quality of life
Renewable energy	Tracking and transparency	Increases transparency, incentivized production, and efficient distribution
Insurance	Risk assessment and fraud detection	Reduces risk, improves accuracy, and streamlines processes

AI, Artificial Intelligence; BCT, blockchain technology; IoT, Internet of things.

➤ **Real-time data processing:** The system emphasizes real-time data processing, enabling swift responses and proactive adjustments based on the insights gleaned from the data.

VII.2 Applications and case studies

Several sectors are transforming because of the convergence of blockchain, IoT, and AI, which is opening new opportunities for accountability, efficiency, and transparency. The transforming potential of this combination is demonstrated by the fascinating case studies and examples of applications detailed in Table 10.

- Supply chain management

Traceability and counterfeiting: Blockchain's immutable ledger provides a tamper-proof record of the journey of goods from their origin to the end

consumer. IoT sensors embedded in products constantly transmit data about their location, condition, and handling to the blockchain, enabling real-time tracking and verification. AI algorithms can analyze these data, identifying potential risks or anomalies and triggering preventative actions. This creates a highly secure and transparent system that can prevent counterfeiting, ensure product quality, and enhance consumer trust. Table 11 gives a detailed overview of the contributions of IoT, blockchain, and AI across various supply chains and industrial applications.

- Healthcare

Secure data sharing and privacy: Blockchain offers a secure and transparent platform for storing and sharing patient data, protecting individual privacy while enabling efficient data access for research and treatment. IoT sensors embedded in medical

Table 11: Contributions of IoT, blockchain, and AI in various supply chains and industrial applications

Case study	Challenge contribution	Blockchain contribution	IoT contribution	AI contribution
[61]	Food safety and traceability	Tracks food product movement	Monitors temperature, humidity, etc.	Identifies risks and alerts stakeholders
[62]	Counterfeiting and drug tampering	Secures transactions and data storage	Monitors drug conditions and location	Analyzes data for risk assessment and process optimization
[59]	- Vaccine quality - Demand forecasting - Trust among stakeholders	Ensures trust among stakeholders	Ensures real-time monitoring of vaccine status	Predicts vaccine demand and conducts sentiment analysis on vaccine reviews
[63]	- Predictive maintenance - Automated response	Provides decentralized trust management and data integrity	Edge devices generate and transmit data	Edge AI algorithms analyze data and enable self-healing actions

AI, Artificial Intelligence; IoT, Internet of things.

Table 12: Contributions of BCT, IoT, and AI in enhancing security and privacy in healthcare

Case study	Challenge addressed	Blockchain contribution	IoT contribution	AI contribution
[64]	Secures patient data management and privacy	Manages and secures patient medical records	Monitors patient vitals and medical information	Personalizes treatment plans and identifies health risks
[65]	Abnormal traffic detection and security	Secures interactive environment for IoMT	Monitors network traffic and device activity	Analyzes traffic patterns and identifies anomalies
[66]	Secures authentication and dynamic attack detection	Provides a secure framework for IoMT authentication	Transmits medical data from devices	Uses KNN algorithm for dynamic time attack detection and authentication
[67]	Secures privacy-preserving data sharing	Provides decentralized data sharing, access control, and model aggregation	Collects data from various sources	Trains ML models on decentralized data

AI, Artificial Intelligence; BCT, blockchain technology; IoMT, Internet of medical things; IoT, Internet of things; ML, machine learning.

devices can continuously monitor patient health, transmitting data to a blockchain-based platform. AI algorithms can then analyze these data to identify potential health risks, personalize treatment plans, and improve patient outcomes. An in-depth overview at how blockchain, IoT, and AI address various challenges is given in Table 12.

- Smart cities

Resource management and optimization: Blockchain, IoT, and AI can work together to optimize resource management and improve efficiency in smart cities. Sensors embedded in traffic lights, waste bins, and energy grids can transmit data to a

Table 13: Contributions of BCT, IoT, and AI in resource optimization and security for smart cities

Case study	Challenge addressed	Blockchain contribution	IoT contribution	AI contribution
[68]	Resource optimization and city management	Manages city infrastructure data	Monitors traffic, energy, and waste	Optimizes resource allocation and efficiency
[6]	Resource management and optimization	Provides secure and decentralized data management for smart city services	Collects data from various sensors in the city	Analyzes data to optimize resource allocation, traffic flow, and energy consumption
[69]	Security, privacy, and trustworthiness	Manages security in smart city infrastructure	Collects data from sensors, devices, and networks	Collects data from sensors, devices, and networks
[5]	Sustainable smart city development	Provides secure and transparent data sharing, decentralized control, and trust	Collects data from various sensors and devices in the city	Analyzes data to optimize resource allocation, improve traffic management, and enhance security

AI, Artificial Intelligence; BCT, blockchain technology; IoT, Internet of things.

blockchain-based platform. AI algorithms can analyze these data to optimize traffic flow, predict waste collection needs, and manage energy consumption more efficiently. This creates a more sustainable and efficient urban environment. A comprehensive summary is given in Table 13.

- Renewable energy

Tracking and transparency: Blockchain can be used to track the origin and flow of renewable energy, ensuring transparency and incentivizing its production and consumption. IoT sensors can monitor the output of solar panels, wind turbines, and other renewable energy sources. AI algorithms can analyze these data to optimize energy production and distribution, ensuring greater efficiency and maximizing the use of renewable resources.

The integration of blockchain and AI in energy cloud management (ECM) is a crucial step toward a more sustainable and efficient energy future, particularly for facilitating the widespread adoption of renewable energy sources. Research (e.g., [70]) highlights the significant role of this integration. It underscores the potential of blockchain to create a secure and transparent environment for P2P energy trading, where prosumers can sell excess energy from their renewable sources (e.g., solar and wind) directly to neighbors, incentivizing renewable energy adoption.

AI algorithms, in turn, can optimize energy production and distribution by accurately predicting demand from renewable sources and facilitating better integration into the grid. This research also emphasizes the need for robust security measures to protect data in blockchain-based energy systems, addressing concerns about data breaches and ensuring the trust and privacy of consumers. Overall, this research contributes to the development of a more secure, transparent, and efficient energy ecosystem that encourages the greater use of renewable energy sources.

VIII Discussion and future search directions

The integration of IoT, blockchain, and AI offers substantial benefits, such as enhanced security, improved decision-making, increased efficiency, increased traceability, and cost reduction. Specific examples from case studies illustrate these benefits clearly. In supply chain management, this technology combination ensures product authenticity and traceability, reducing fraud and increasing stakeholder trust. Healthcare can benefit from secure and accurate patient data, leading to better diagnostics and personalized treatment plans. Smart cities can enhance infrastructure management and service delivery, while renewable energy sectors can optimize

energy usage and improve grid management through real-time data and predictive maintenance. These applications demonstrate the potential of integrating IoT, blockchain, and AI to address specific challenges and drive efficiency across various sectors.

However, several challenges must be addressed to fully realize the potential of integrating IoT, blockchain, and AI. Data complexity and interoperability issues arise from integrating blockchain's decentralized data structure with AI systems that require structured and standardized data. Scalability is another significant challenge, as blockchain platforms currently struggle with handling the vast amounts of data needed for AI systems. The limited transaction processing capacity and data storage capabilities of existing BCT pose barriers, necessitating research into scalable blockchain architectures and efficient data management strategies. Security and privacy concerns also emerge from the integration of AI and blockchain, highlighting the need for secure AI algorithms, robust cryptography techniques, and privacy-preserving data analysis approaches. Additionally, transparency and explainability in AI systems are crucial, especially when combined with blockchain, to ensure that AI models are auditable and understandable.

Establishing clear regulatory frameworks is crucial for governing the building and implementation of AI-powered blockchain systems. Guidelines for data privacy, security, and responsible AI usage are necessary to ensure that these technologies are developed and implemented ethically and safely. Policymakers, researchers, and industry experts must collaborate to create regulations that foster innovation while protecting public interests. Despite the challenges, the future of this technological integration is promising, with continuous advancements expected to address current limitations. Encouraging further research and development in areas like data complexity, scalability, security, transparency, and regulatory frameworks is crucial. Collaboration among stakeholders will drive innovation and effectively address societal challenges, fully realizing the transformative potential of IoT, blockchain, and AI integration.

However, several limitations of this study must be acknowledged to provide a balanced perspective. First, the rapid evolution of IoT, blockchain, and AI technologies means that some of the solutions and challenges discussed may become obsolete or less relevant over time. Furthermore, the scope of the survey may not cover all possible applications and sectors where these technologies intersect, potentially missing important contexts and developments.

Another limitation is the variability in the maturity and adoption rates of these technologies across different regions and industries, which may affect the generalizability of the results. Furthermore, the study relies heavily on existing literature and case studies, which may introduce biases or gaps if certain aspects of technology integration have not been widely explored or reported. Finally, practical implementation aspects, such as cost, resource availability, and the readiness of existing infrastructure, are not analyzed in depth, which could impact the feasibility of the proposed solutions in real-world scenarios. Addressing these limitations in future research will be essential to fully exploit the potential benefits of integrating IoT, blockchain, and AI technologies.

To provide a more structured roadmap for future research, it is essential to detail specific technical, application, and policy areas that require attention. From a technical point of view, it is also very important to establish standardized protocols for exchanging data between blockchain and AI systems to resolve issues of complexity and interoperability. Existing blockchain platforms suffer from the sheer volume of information needed by their AIs because of the decentralized structure and this is an important area for development. Furthermore, the investigation of new blockchain environments capable of processing and storing the massive quantities of data produced by AI applications is also desirable. Such frameworks should aim at increasing both the transaction rate processing and data storage capacity of BCT, either by using new approaches like sharding or layered ones. Additionally, cryptographic innovation to enhance data protection and privacy in embedded systems is essential. This also encompasses the design of optimized cryptographic algorithms to secure AI models and their associated data while providing high efficiency and performance.

On the application side, it is important to develop case studies and pilot projects in key sectors to demonstrate practical benefits and guide future implementations. For example, in supply chain management, creating pilot projects integrating IoT, blockchain, and AI can provide concrete evidence of improved product authenticity, improved traceability, and reduced fraud. In healthcare, developing secure and interoperable platforms for patient data management can leverage blockchain for data integrity and AI for diagnostic support, leading to better patient outcomes. Also, in the smart city infrastructure context, it can be advantageous to investigate AI and blockchain technologies to help optimize infrastructure management, service provision, and civic

engagement by leveraging enhanced data analytics and automation.

Concerning a policy standpoint, it is crucial to put in place integrative legislation covering data privacy, security, and ethical application of AI. These rules need to guarantee responsible and ethical development and implementation of such technologies that protect public interests and encourage innovation. Efforts to encourage partnerships between policy-makers, industry practitioners, and scientists are crucial for developing policies that encourage technological innovation but are also relevant to social issues. Although this collaboration can support an initial set of best practices and guidelines for the transparency and explainability of AI systems, particularly in the context of BCT where AI models are verifiable and understandable, not all stakeholders necessarily support this effort. Addressing these technical, application-oriented, and policy-related issues, this systematic roadmap is intended to address the present challenges and deliver in full its promise regarding the co-integration of IoT, blockchain, and AI in different fields and contribute to innovation and societal value.

IX Conclusion

The integration of IoT, blockchain, and AI holds immense potential to transform various sectors, enhancing security, efficiency, and transparency in data management and decision-making. This convergence creates a robust ecosystem with significant benefits, including enhanced data security, improved decision-making, increased efficiency, increased traceability, and cost reduction. This study highlights real-world applications across supply chain management, healthcare, smart cities, and renewable energy, demonstrating the practical benefits of this integration.

However, challenges, such as data complexity, scalability, security, explainability, and regulatory frameworks, require further research and development. Addressing these challenges is crucial for ensuring the successful adoption and implementation of these technologies. Collaboration between researchers, industry experts, and policymakers is vital for developing solutions that promote innovation and protect public interests. The future of this integration is promising, with continuous advancements expected in the technologies, particularly in addressing scalability and security concerns. As research and development continue, the convergence of IoT, blockchain, and AI will play a pivotal role in shaping a more efficient, secure, and sustainable future.

References

- [1] S. Choudhary and G. Meena, "Internet of Things: Protocols, Applications and Security Issues," *Procedia Computer Science*, vol. 215, pp. 274–288, 2022, doi: 10.1016/j.procs.2022.12.030.
- [2] A. Miglani and N. Kumar, "Blockchain management and machine learning adaptation for IoT environment in 5G and beyond networks: A systematic review," *Computer Communications*, vol. 178, no. July 2021, pp. 37–63, 2021, doi: 10.1016/j.comcom.2021.07.009.
- [3] P. Bothra, R. Karmakar, S. Bhattacharya, and S. De, "How can applications of blockchain and artificial intelligence improve performance of Internet of Things? – A survey," *Computer Networks*, vol. 224, no. May 2021, p. 109634, 2023, doi: 10.1016/j.comnet.2023.109634.
- [4] V. V. Prabhakar, C. S. Belarmin Xavier, and K. M. Abubeker, "A Review on Challenges and Solutions in the Implementation of Ai, IoT and Blockchain in Construction Industry," *Materials Today: Proceedings*, 2023, doi: 10.1016/j.matpr.2023.03.535.
- [5] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I. H. Ra, "Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city," *Sustainable Cities and Society*, vol. 63, no. April, 2020, doi: 10.1016/j.scs.2020.102364.
- [6] A. Kumari, R. Gupta, and S. Tanwar, "Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review," *Computer Communications*, vol. 172, no. October 2020, pp. 102–118, 2021, doi: 10.1016/j.comcom.2021.03.005.
- [7] E. Fazel, M. Z. Nezhad, J. Rezazadeh, M. Moradi, and J. Ayoade, "IoT convergence with machine learning & blockchain: A review," *Internet of Things (Netherlands)*, vol. 26, no. December 2023, p. 101187, 2024, doi: 10.1016/j.iot.2024.101187.
- [8] N. S. Al-Blihed, N. F. Al-Mufadi, N. T. Al-Harbi, I. A. Al-Omari, and M. A. Al-Hagery, "Blockchain and machine learning in the internet of things: a review of smart healthcare," *IAES International Journal of Artificial Intelligence*, vol. 12, no. 3, pp. 995–1006, 2023, doi: 10.11591/ijai.v12.i3.pp995-1006.
- [9] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things (Netherlands)*, vol. 11, p. 100227, 2020, doi: 10.1016/j.iot.2020.100227.
- [10] T. Nguyen, H. Nguyen, and T. Nguyen Gia, "Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security,

and applications,” *Journal of Network and Computer Applications*, vol. 226, no. September 2023, p. 103884, 2024, doi: 10.1016/j.jnca.2024.103884.

[11] A. M. Shamsan Saleh, “Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review,” *Blockchain: Research and Applications*, p. 100193, 2024, doi: 10.1016/j.bcra.2024.100193.

[12] P. Pandurangan et al., “Integrating cutting-edge technologies: AI, IoT, blockchain and nanotechnology for enhanced diagnosis and treatment of colorectal cancer - A review,” *Journal of Drug Delivery Science and Technology*, vol. 91, no. August 2023, p. 105197, 2024, doi: 10.1016/j.jddst.2023.105197.

[13] Z. Kamal, M. Lachgar, and H. Hrimech, “Blockchain, IoT and AI in logistics and transportation : A systematic review,” *Transport Economics and Management*, vol. 2, no. July, pp. 275–285, 2024, doi: 10.1016/j.team.2024.09.002.

[14] M. Gupta, M. Kumar, and R. Dhir, “Unleashing the prospective of blockchain-federated learning fusion for IoT security: A comprehensive review,” *Computer Science Review*, vol. 54, no. June, p. 100685, 2024, doi: 10.1016/j.cosrev.2024.100685.

[15] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” vol. 15, no. 4, pp. 580–596, 2008.

[16] M. Pasqua, A. Benini, F. Contro, M. Crosara, and M. D. Preda, “Enhancing Ethereum smart-contracts static analysis by computing a precise Control-Flow Graph of Ethereum bytecode,” *The Journal of Systems & Software*, vol. 200, p. 111653, 2023, doi: 10.1016/j.jss.2023.111653.

[17] T. Guimarães^a et al., “Blockchain Analytics - Real-time Log Management in Healthcare Blockchain Analytics - Real-time Log Management in Healthcare,” vol. 00, 2022, doi: 10.1016/j.procs.2022.03.094.

[18] B. Bhushan, A. Khamparia, K. M. Sagayam, S. K. Sharma, M. A. Ahad, and N. C. Debnath, “Blockchain for smart cities: A review of architectures, integration trends and future research directions,” *Sustainable Cities and Society*, vol. 61, no. March, p. 102360, 2020, doi: 10.1016/j.scs.2020.102360.

[19] Y. Shen and X. Zhang, “Factors influencing blockchain adoption in supply chain management practices: A study based on the oil industry,” *Journal of Innovation & Knowledge*, vol. 8, no. 3, p. 100384, 2023, [Online]. Available: DOI: 10.1016/j.jik.2023.100384.

[20] G. Tripathi, M. A. Ahad, and G. Casalino, “A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges,” *Decision Analytics Journal*, vol. 9, no. March, p. 100344, 2023, doi: 10.1016/j.dajour.2023.100344.

[21] M. R. Islam, M. M. Rahman, M. Mahmud, M. A. Rahman, M. H. S. Mohamad, and A. H. Embong, “A Review on Blockchain Security Issues and Challenges,” *2021 IEEE 12th Control and System Graduate Research Colloquium, ICSGRC 2021 - Proceedings*, no. August, pp. 227–232, 2021, doi: 10.1109/ICSGRC53186.2021.9515276.

[22] D. R. Kiran, “Chapter 35 - Internet of Things,” in *Production Planning and Control*, D. R. Kiran, Ed. Butterworth-Heinemann, 2019, pp. 495–513.

[23] E. Gelenbe, M. Nakip, and T. Czachórski, “Improving Massive Access to IoT Gateways,” *Performance Evaluation*, vol. 157–158, p. 102308, 2022, doi: 10.1016/j.peva.2022.102308.

[24] C. K. Rath, A. K. Mandal, and A. Sarkar, “Microservice based scalable IoT architecture for device interoperability,” *Computer Standards and Interfaces*, vol. 84, no. October 2022, 2023, doi: 10.1016/j.csi.2022.103697.

[25] S. Rudrakar and P. Rughani, “IoT based Agriculture (Ag-IoT): A detailed study on Architecture, Security and Forensics,” *Information Processing in Agriculture*, no. August, 2023, doi: 10.1016/j.inpa.2023.09.002.

[26] L. Yang and A. Shami, “IoT data analytics in dynamic environments: From an automated machine learning perspective,” *Engineering Applications of Artificial Intelligence*, vol. 116, no. August, p. 105366, 2022, doi: 10.1016/j.engappai.2022.105366.

[27] P. Akhtar, Z. Khan, S. Tarba, and U. Jayawickrama, “The Internet of Things, dynamic data and information processing capabilities, and operational agility,” *Technological Forecasting and Social Change*, vol. 136, no. May 2017, pp. 307–316, 2018, doi: 10.1016/j.techfore.2017.04.023.

[28] I. H. Sarker, “Machine Learning: Algorithms, Real-World Applications and Research Directions,” *SN Computer Science*, vol. 2, no. 3, pp. 1–21, 2021, doi: 10.1007/s42979-021-00592-x.

[29] A. U. Osarogiagbon, F. Khan, R. Venkatesan, and P. Gillard, “Review and analysis of supervised machine learning algorithms for hazardous events in drilling operations,” *Process Safety and Environmental Protection*, vol. 147, pp. 367–384, 2021, doi: 10.1016/j.psep.2020.09.038.

[30] D. del-Pozo-Bueno, D. Kepaptsoglou, F. Peiró, and S. Estradé, “Comparative of machine learning classification strategies for electron energy loss spectroscopy: Support vector machines and artificial neural networks,” *Ultramicroscopy*, vol. 253, no. July, 2023, doi: 10.1016/j.ultramic.2023.113828.

[31] K. Hu et al., “A review of research on reinforcement learning algorithms for multi-agents,”

Neurocomputing, vol. 599, no. November 2023, p. 128068, 2024, doi: 10.1016/j.neucom.2024.128068.

[32] N. S. A. Polireddi, "An effective role of artificial intelligence and machine learning in banking sector," *Measurement: Sensors*, vol. 33, no. November 2023, p. 101135, 2024, doi: 10.1016/j.measen.2024.101135.

[33] B. Abdualgalil and S. Abraham, "Applications of Machine Learning Algorithms and Performance Comparison: A Review," *International Conference on Emerging Trends in Information Technology and Engineering, ic-ETITE 2020*, pp. 1–6, 2020, doi: 10.1109/ic-ETITE47903.2020.490.

[34] D. D. Nguyen and M. I. Ali, "Enabling On-demand decentralized IoT collectability marketplace using blockchain and crowdsensing," *Global IoT Summit, GloTS 2019 - Proceedings*, pp. 1–6, 2019, doi: 10.1109/GIOTS.2019.8766346.

[35] C. Liu, Y. Xiao, V. Javangula, Q. Hu, S. Wang, and X. Cheng, "NormaChain: A blockchain-based normalized autonomous transaction settlement system for IoT-based e-commerce," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4680–4693, 2019, doi: 10.1109/JIOT.2018.2877634.

[36] Q. Ren, K. L. Man, M. Li, and B. Gao, "Using Blockchain to Enhance and Optimize IoT-based Intelligent Traffic System," *2019 International Conference on Platform Technology and Service, PlatCon 2019 - Proceedings*, pp. 1–4, 2019, doi: 10.1109/PlatCon.2019.8669412.

[37] W. Liang, L. You, and G. Hu, "LRS_PKI: A novel blockchain-based PKI framework using linkable ring signatures," *Computer Networks*, vol. 237, no. August, p. 110043, 2023, doi: 10.1016/j.comnet.2023.110043.

[38] S. Khanji, O. Alfandi, L. Ahmad, L. Kakkengal, and M. Al-kfairy, "A systematic analysis on the readiness of Blockchain integration in IoT forensics," *Forensic Science International: Digital Investigation*, vol. 42–43, p. 301472, 2022, doi: 10.1016/j.fsidi.2022.301472.

[39] A. Tomar, N. Gupta, D. Rani, and S. Tripathi, "Blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system," *Internet of Things (Netherlands)*, vol. 23, no. June, p. 100849, 2023, doi: 10.1016/j.iot.2023.100849.

[40] S. Brotsis *et al.*, "Blockchain meets Internet of Things (IoT) forensics: A unified framework for IoT ecosystems," *Internet of Things (Netherlands)*, vol. 24, no. August, p. 100968, 2023, doi: 10.1016/j.iot.2023.100968.

[41] X. Lu, "Implementation of art therapy assisted by the internet of medical things based on blockchain and fuzzy set theory," *Information Sciences*, vol.

632, no. March, pp. 776–790, 2023, doi: 10.1016/j.ins.2023.03.044.

[42] D. Kumar, R. K. Singh, R. Mishra, and T. U. Daim, "Roadmap for integrating blockchain with Internet of Things (IoT) for sustainable and secured operations in logistics and supply chains: Decision making framework with case illustration," *Technological Forecasting and Social Change*, vol. 196, no. September, p. 122837, 2023, doi: 10.1016/j.techfore.2023.122837.

[43] H. Nguyen, D. Nawara, and R. Kashef, "Connecting the indispensable roles of IoT and artificial intelligence in smart cities: A survey," *Journal of Information and Intelligence*, no. December 2023, pp. 1–25, 2024, doi: 10.1016/j.jiixd.2024.01.003.

[44] W. S. Costa *et al.*, "Planning and resource allocation of a hybrid IoT network using artificial intelligence," *Internet of Things (Netherlands)*, vol. 26, no. April, p. 101225, 2024, doi: 10.1016/j.iot.2024.101225.

[45] K. Alpan, K. Tuncal, C. Ozkan, B. Sekeroglu, and Y. K. Ever, "Design and simulation of global model for carbon emission reduction using IoT and artificial intelligence," *Procedia Computer Science*, vol. 204, pp. 627–634, 2022, doi: 10.1016/j.procs.2022.08.076.

[46] A. A. Malibari, "An efficient IoT-Artificial intelligence-based disease prediction using lightweight CNN in healthcare system," *Measurement: Sensors*, vol. 26, no. October 2022, p. 100695, 2023, doi: 10.1016/j.measen.2023.100695.

[47] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020, doi: 10.1109/COMST.2020.2986444.

[48] F. Alwahedi, A. Aldaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," *Internet of Things and Cyber-Physical Systems*, vol. 4, no. August 2023, pp. 167–185, 2024, doi: 10.1016/j.iotcps.2023.12.003.

[49] T. Mazhar *et al.*, "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence," *Brain Sciences*, vol. 13, no. 4, 2023, doi: 10.3390/brainsci13040683.

[50] S. Vyas, M. Gupta, and R. Yadav, "Converging Blockchain and Machine Learning for Healthcare," *Proceedings - 2019 Amity International Conference on Artificial Intelligence, AICAI 2019*, pp. 709–711, 2019, doi: 10.1109/AICAI.2019.8701230.

[51] P. Singh, Z. Elmi, Y. yip Lau, M. Borowska-Stefańska, S. Wiśniewski, and M. A. Dulebenets,

- "Blockchain and AI technology convergence: Applications in transportation systems," *Vehicular Communications*, vol. 38, no. 2022, 2022, doi: 10.1016/j.vehcom.2022.100521.
- [52] M. Soori, R. Dastres, and B. Arezoo, "AI-powered blockchain technology in industry 4.0, a review," *Journal of Economy and Technology*, vol. 1, no. November 2023, pp. 222–241, 2023, doi: 10.1016/j.ject.2024.01.001.
- [53] H. Y. Chen, K. Sharma, C. Sharma, and S. Sharma, "Integrating explainable artificial intelligence and blockchain to smart agriculture: Research prospects for decision making and improved security," *Smart Agricultural Technology*, vol. 6, no. November, p. 100350, 2023, doi: 10.1016/j.atech.2023.100350.
- [54] D. Bhumichai, C. Smiliotopoulos, R. Benton, G. Kambourakis, and D. Damopoulos, "The Convergence of Artificial Intelligence and Blockchain: The State of Play and the Road Ahead," *Information (Switzerland)*, vol. 15, no. 5, pp. 1–32, 2024, doi: 10.3390/info15050268.
- [55] D. Ressi, R. Romanello, C. Piazza, and S. Rossi, "AI-enhanced blockchain technology: A review of advancements and opportunities," *Journal of Network and Computer Applications*, vol. 225, no. May 2023, p. 103858, 2024, doi: 10.1016/j.jnca.2024.103858.
- [56] O. Popoola, M. Rodrigues, J. Marchang, A. Shenfield, A. Ikpehia, and J. Popoola, "A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: Problems, Challenges and Solutions," *Blockchain: Research and Applications*, vol. 5, no. 2, p. 100178, 2023, doi: 10.1016/j.bcra.2023.100178.
- [57] P. Nath, J. R. Mushahary, U. Roy, M. Brahma, and P. K. Singh, "AI and Blockchain-based source code vulnerability detection and prevention system for multiparty software development," *Computers and Electrical Engineering*, vol. 106, no. June 2022, p. 108607, 2023, doi: 10.1016/j.compeleceng.2023.108607.
- [58] S. M. Alrubei, E. Ball, and J. M. Rigelsford, "A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer," *IEEE Access*, vol. 10, pp. 18583–18595, 2022, doi: 10.1109/ACCESS.2022.3151370.
- [59] H. Hu, J. Xu, M. Liu, and M. K. Lim, "Vaccine supply chain management: An intelligent system utilizing blockchain, IoT and machine learning," *Journal of Business Research*, vol. 156, no. December 2022, p. 113480, 2023, doi: 10.1016/j.jbusres.2022.113480.
- [60] S. K. Singh, S. Rathore, and J. H. Park, "BlockIoTelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence," *Future Generation Computer Systems*, vol. 110, pp. 721–743, 2020, doi: 10.1016/j.future.2019.09.002.
- [61] M. Lei, L. Xu, T. Liu, S. Liu, and C. Sun, "Integration of Privacy Protection and Blockchain-Based Food Safety Traceability: Potential and Challenges," *Foods*, vol. 11, no. 15, 2022, doi: 10.3390/foods11152262.
- [62] N. Mangala et al., "Secure pharmaceutical supply chain using blockchain in IoT cloud systems," *Internet of Things (Netherlands)*, vol. 26, no. April, p. 101215, 2024, doi: 10.1016/j.iot.2024.101215.
- [63] X. Feng, J. Wu, Y. Wu, J. Li, and W. Yang, "Blockchain and digital twin empowered trustworthy self-healing for edge-AI enabled industrial Internet of things," *Information Sciences*, vol. 642, no. May, p. 119169, 2023, doi: 10.1016/j.ins.2023.119169.
- [64] W. Moulahi, I. Jdey, T. Moulahi, M. Alawida, and A. Alabdulatif, "A blockchain-based federated learning mechanism for privacy preservation of health-care IoT data," *Computers in Biology and Medicine*, vol. 167, no. June, p. 107630, 2023, doi: 10.1016/j.combiomed.2023.107630.
- [65] J. Wang, H. Jin, J. Chen, J. Tan, and K. Zhong, "Anomaly detection in Internet of medical Things with Blockchain from the perspective of deep neural network," *Information Sciences*, vol. 617, pp. 133–149, 2022, doi: 10.1016/j.ins.2022.10.060.
- [66] Y. D. Al-Otaibi, "K-nearest neighbour-based smart contract for internet of medical things security using blockchain," *Computers and Electrical Engineering*, vol. 101, no. May, p. 108129, 2022, doi: 10.1016/j.compeleceng.2022.108129.
- [67] A. Zekiye and Ö. Özkasap, "Decentralized Healthcare Systems with Federated Learning and Blockchain," 2023, [Online]. Available: <http://arxiv.org/abs/2306.17188>.
- [68] I. Ahmed, Y. Zhang, G. Jeon, W. Lin, M. R. Khosravi, and L. Qi, "A blockchain- and artificial intelligence-enabled smart IoT framework for sustainable city," *International Journal of Intelligent Systems*, vol. 37, no. 9, pp. 6493–6507, 2022, doi: 10.1002/int.22852.
- [69] A. Shankar and C. Maple, "Securing the Internet of Things-enabled smart city infrastructure using a hybrid framework," *Computer Communications*, vol. 205, no. August 2022, pp. 127–135, 2023, doi: 10.1016/j.comcom.2023.04.008.
- [70] A. Kumari, R. Gupta, S. Tanwar, and N. Kumar, "Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions," *Journal of Parallel and Distributed Computing*, vol. 143, pp. 148–166, 2020, doi: 10.1016/j.jpdc.2020.05.004.