Survey on the Adoption of Blockchain Technology in Internet of Things Environments: Techniques, Challenges and Future Research Directions

Zouhair Elhadari, Hicham Zougagh, Noureddine Idboufker, Mohamed Ech-chebaby

***Abstract*— Blockchain has recently garnered considerable attention in academic research across various fields. In the Internet of Things (IoT) domain, blockchain is viewed as a tool for establishing a decentralized, reliable, and secure environment. However, its application in IoT, especially for smaller-scale systems, is still nascent. Consequently, the future direction of blockchain in IoT remains somewhat uncertain, with numerous challenges and unresolved questions. Although many articles have explored the intersection of blockchain technology and IoT, most offer only surface-level discussions on the technological potential, with few addressing the complexities of implementing blockchain in IoT environments. This paper aims to provide a coherent and comprehensive overview of current leading efforts in this area. Specifically, we survey the integration of IoT and blockchain by examining key research themes and trends in blockchain-related methodologies and technologies applied to IoT. In this study, we reviewed articles published between 2021 and 2023 on blockchain-based IoT solutions, categorizing them into distinct research areas. We aim to explore the technologies, benefits, issues, and challenges related to the integration of IoT and blockchain, while also investigating the efforts made to address these challenges.**

***Index Terms*— Blockchain, Internet of things, IoT, Integration of blockchain with IoT, adoption of blockchain in IoT, Blockchain challenges, Survey.**

I. Introduction

In the realm of private and secure data management, blockchain technology has emerged as one of the most effective solutions due to its inherent properties, such as immutability and irreversibility. Blockchain ensures data integrity by preventing unauthorized modifications. When changes are made to the distributed ledger through transactions, these updates are propagated to all nodes in the network, which independently verify and update their respective copies. Once a transaction is validated across the network, altering it becomes virtually impossible without modifying both the preceding and subsequent blocks. Consequently, blockchain transactions are irreversible, and new data is continually appended to the chain. Each block is cryptographically linked to its predecessor, forming a chain that can be traced in reverse chronological order. The unique capabilities of blockchain arise from its decentralized, distributed structure, enhanced by robust cryptographic techniques.

This technology is particularly advantageous in scenarios demanding high levels of security and confidentiality, such as the IoT. The IoT field is witnessing unprecedented growth, with estimates suggesting the deployment of nearly 30 billion interconnected devices by 2025.

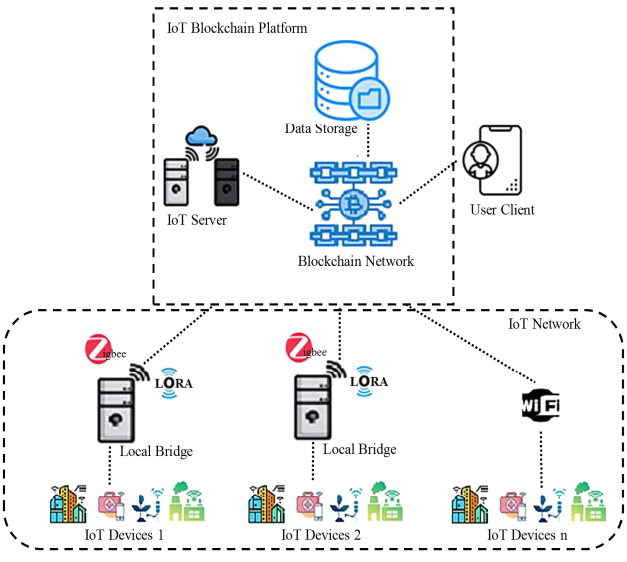

Fig1: Integration of blockchain technology in the IoT environment

Manuscript received March 11, 2024; revised November 20, 2024.

Zouhair Elhadari is a Ph.D. student in the Department of Computer Science, Faculty of Sciences and Techniques, Moulay Slimane University, Beni Mellal, Morocco. (email: zouhair.hdr@gmail.com).

Hicham Zougagh is a full Professor in the Department of Computer Science, Faculty of Sciences and Techniques, Moulay Slimane University, Beni Mellal, Morocco. (email: h.zougagh@usms.ma).

Noureddine Idboufker is a full Professor in the Department of Telecommunications and Computer Sciences, National School of Applied Sciences, Cady Ayyad University, Marrakech, Morocco. (email: n_idboufker@yahoo.fr).

Mohamed Ech-chebaby is a Ph.D. student in the Department of Computer Science, Faculty of Sciences and Techniques, Moulay Slimane University, Beni Mellal, Morocco. (email: med.echchebaby@gmail.com).

However, this rapid expansion introduces significant cybersecurity challenges, as IoT devices are increasingly vulnerable to various forms of cyberattacks. Conventional security models, which rely on centralized architectures, leave IoT devices susceptible to malicious intrusions. The convergence of IoT and blockchain technology offers a promising approach to strengthening the security of the IoT ecosystem, as will be explored in the subsequent sections.

A. Scope of this survey

Based on the scope of this survey, the focus is on integrating blockchain technology into IoT environments, addressing key aspects such as security, privacy, data integrity, access control, and the development of new architectures. The survey covers the following areas of research:

In [1]–[10], the authors examine how blockchain technology can enhance security and privacy in IoT systems. This includes ensuring data integrity, access control, and management, as well as developing new architectures for smart home IoT systems.

In [11]–[20], the authors explore the development of decentralized and scalable solutions for smart cities' IoT environments using blockchain technology. Topics include secure data collection, continuous delivery, methods for continuous verification of IoT data flows, and improvements in security, interoperability, and data exchange.

In [21]–[30], the research focuses on improving efficiency, reliability, and security in healthcare IoT systems. This includes remote patient monitoring, secure health data sharing, lightweight access control, and the development of secure frameworks for healthcare systems.

The authors of [31]–[40] address challenges related to the integration of blockchain with the Industrial Internet of Things (IIoT). Key topics include solutions for storage, latency, reliability, scalability, privacy, and security. Additionally, this research emphasizes ensuring data integrity and authenticity to enhance network performance and lifespan.

In [41]–[50], the authors investigate how blockchain technology can improve data collection, management, and sharing in supply chains and smart agriculture systems. Their focus is on enhancing transparency, traceability, and automating business processes.

Finally, in [51]–[60], the authors discuss the development of new architectures to address bandwidth constraints and trust issues in centralized systems. They also examine improving privacy in 5G networks, enhancing transparency and security in energy trading, and managing trust in IoT smart energy environments using blockchain.

This survey aims to provide a comprehensive overview of the integration of blockchain technology into various IoT domains, highlighting its potential to address a wide range of challenges and improve the overall performance, security, and privacy of IoT systems.

B. Contribution of this survey

This survey, which focuses on the integration of blockchain technology into IoT environments with an emphasis on security, privacy, data integrity, access control, and architectural development, highlights the following key research contributions:

1) Comprehensive Review: This survey provides a systematic and in-depth review of the IoT paradigm and blockchain technology, exploring its applications across various IoT domains.
2) Application Insights: The survey discusses diverse applications and technologies related to integrating blockchain into IoT systems across different fields, including smart homes, smart cities, healthcare, IIoT, smart agriculture, and smart energy.
3) Addressing Research Challenges: This survey addresses existing gaps in the research regarding security, privacy, scalability, interoperability, and other challenges associated with implementing blockchain technology in IoT environments.

The primary objective of this survey is to provide a holistic understanding of how blockchain technology can be integrated into various IoT domains, with the goal of overcoming a wide range of challenges and improving the performance, security, and privacy of IoT systems.

C. Organization and reading map

This work is organized as follows: Section 1 presents the introduction, outlining the scope and contributions of this survey. Section 2 provides an overview of related work. In Section 3, we present a detailed review of the key principles and operation of blockchain technology and the IoT, along with the various application areas where blockchain is applied within the IoT. Section 4 explains the methodology used to select and analyze the papers discussed in this survey. This includes details about the search strategy, the criteria for determining eligibility, the selection process results, and the key attributes of the included articles. Section 5 focuses on presenting the methods, benefits, and limitations of previous research regarding the integration of blockchain technology into multiple IoT environments. Section 6 addresses the challenges and future research directions in this area. Finally, Section 7 concludes the work with final remarks.

II. Related work

A significant amount of research has emerged on the integration of blockchain technology into IoT environments. This section briefly summarizes relevant surveys on the topic. The following works provide insightful studies:

Md Ashraf Uddin et al. [61] examine how blockchain can be integrated into IoT systems to tackle issues such as privacy concerns, single points of failure, and data bottlenecks. They review recent advancements in blockchain applications across various IoT fields, including eHealth and smart cities, while discussing the challenges and potential solutions in this context.

Elhama Shammar et al. [62] explore blockchain's integration with IoT from a security perspective, reviewing research from 2017 to 2021. Their study categorizes articles by security areas and provides a comprehensive overview of current efforts and challenges in securing IoT environments using blockchain technology.

Alia Al Sadawi et al. [63] discuss how blockchain can enhance IoT systems in terms of security, authenticity, reliability, and scalability. They explore blockchain's role in improving data storage, processing, security, and

authentication in IoT, and propose an architectural design for integrating these technologies.

Abdelzahir Abdelmaboud et al. [64] provide a thorough overview of how blockchain can solve issues related to scalability, interoperability, security, privacy, and trust in IoT applications. They present a taxonomy of blockchain applications in IoT, discuss popular platforms, and outline the latest advances and challenges for future research.

Ahmed Alkhateeb et al. [65] investigate the use of hybrid blockchain platforms for IoT. They discuss the motivations behind adopting hybrid platforms, the technologies involved, and the challenges they face, highlighting both the advantages and obstacles in implementing hybrid blockchain solutions.

Rajesh Kumar and Rewa Sharma [66] examine blockchain's role in enhancing trust in IoT systems. They provide an overview of IoT and blockchain, discuss trust-related challenges, and compare traditional and blockchain-based trust management techniques.

Haider Dhia Zubaydi et al. [67] conduct a systematic literature review on the integration of blockchain and IoT to address security and privacy issues. Their review covers the benefits of improved security and anonymity, challenges such as storage capacity and legal issues, and future research directions in this domain.

Sarvesh Tanwar et al. [68] explore blockchain's potential to improve IoT security and privacy. They review current research, highlight challenges, and discuss how blockchain's security features can address vulnerabilities in IoT systems.

Vinay Gugueoth et al. [69] investigate the security and privacy challenges in IoT and how decentralized blockchain techniques can address them. Their study covers security threats, blockchain solutions, consensus protocols, and the challenges of integrating blockchain into IoT, offering insights into future research opportunities.

III. Basics of Blockchain and IoT (Overview)

In this section, we present an overview of the Internet of Things (IoT) and blockchain technology, including aspects such as architectural design, characteristics, protocols, consensus algorithms, and blockchain types.

A. Blockchain technology

1) Architecture

A blockchain is a chronologically ordered sequence of immutable transactions managed by a decentralized network of computers utilizing consensus algorithms. Each participating computer in this network, referred to as a "node," maintains an identical copy of the data, known as the "digital ledger" [65], [70].

The ledger is organized into a series of consecutive blocks, and all nodes use the same consensus algorithm to reach an agreement on the validity of transactions. These transactions are stored across all nodes in a distributed Peer-to-Peer (P2P) network [67].

Figure 2 illustrates the general structure of a blockchain, highlighting its fundamental block components. Each block contains the following elements [62], [66] :

Version Information: Indicates the version of the blockchain protocol, used to track updates and changes throughout the protocol's lifespan.

Nonce Value: A randomly generated number that miners seek to find during the mining process. It is crucial in solving the cryptographic puzzle needed to validate the block.

Hash Value of the Previous Block: A cryptographic hash of the preceding block, ensuring each block is securely linked to its predecessor, thereby maintaining the chain's immutability.

Timestamp: Records the time a transaction was added, establishing a chronological order for the transactions.

Merkle Root: A hash derived from the individual transaction hashes within the block, summarizing all the transactions and ensuring both efficiency and security.

Transactions: A list of the individual transactions contained within the block, with details like sender, receiver, and transaction amount.

Thus, a blockchain is made up of a decentralized network of nodes working together through a consensus algorithm to maintain an immutable ledger of timestamped transactions organized in sequential blocks. The chain’s integrity and security are upheld through cryptographic hashing, with each block containing essential components such as version information, nonce value, the previous block’s hash, timestamp, Merkle root, and a list of transactions.

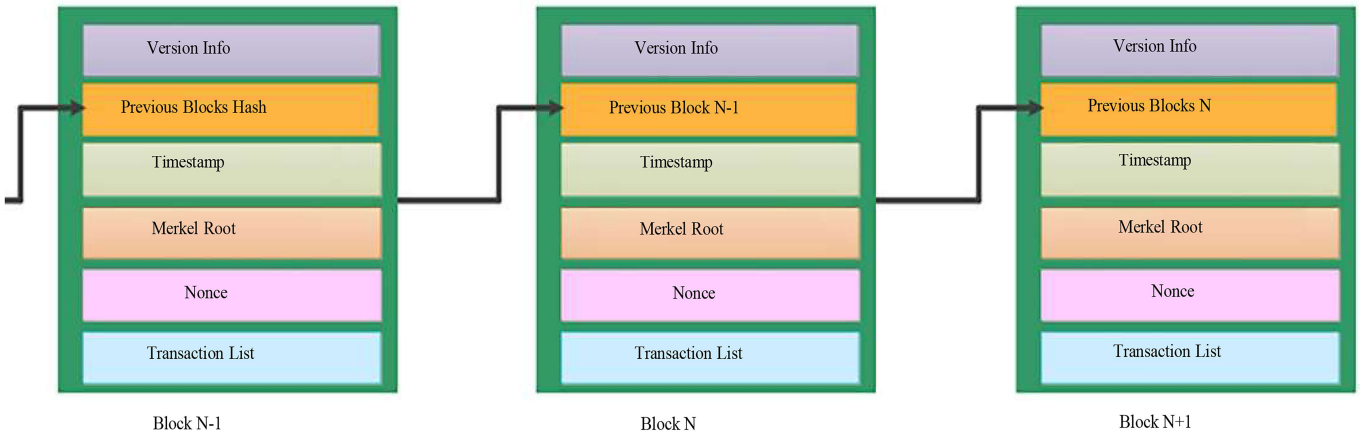

Fig 2: Blockchain structure.

2) Characteristics

Below are the main characteristics of blockchain that contribute to its powerful applications [63], [64] :

Decentralization: Blockchain operates in a decentralized framework, with multiple nodes responsible for managing and maintaining the network. Unlike centralized systems such as traditional banks, where control is in the hands of a single entity, each node in a blockchain network holds an identical copy of the digital ledger. This decentralization significantly increases the cost of hacking, making it a key feature for enhancing the security of blockchain-enabled environments.

Immutability: Blockchain represents a permanent and unalterable network of interconnected nodes. Every node holds a copy of the ledger, and any transaction must undergo authentication and verification before being added to the chain. This results in data being highly resistant to tampering due to the strong protections offered by the network. As a result, blockchain ensures a transparent and secure system where transactions are visible to all but cannot be altered or deleted.

Automation: Blockchain utilizes smart contracts to expedite transaction processing. Smart contracts are digital agreements that self-execute once predefined conditions are met. This automation enables faster, more efficient transactions by eliminating the need for intermediaries and manual oversight.

Transparency: Blockchain provides unmatched transparency, which is crucial for advanced data security solutions. Transactions in the decentralized network are validated by the majority of nodes, allowing users to view real-time updates while maintaining full transparency across the network. This openness ensures the integrity of the data.

Security: Blockchain ensures security through encryption of chain addresses and a consensus process that guarantees data integrity. Transactions and contracts recorded on the blockchain are secure, simplifying IoT protocols. In contrast to centralized systems, blockchain provides stronger protection against piracy. Its distributed nature, along with the use of cryptographic hash functions, makes forging data nearly impossible, ensuring the integrity of transaction histories and defending against malicious threats.

Trust: Blockchain enhances trust by creating a decentralized, tamper-resistant record of transactions, removing the need for centralized authorities. Smart contracts automate the execution of agreements, further establishing trust among parties. In the IoT context, blockchain provides reliable transactions, secure data management, and device identity validation, strengthening trust in IoT networks.

Privacy: Privacy is a critical challenge in IoT applications, particularly when handling sensitive data such as in healthcare. While blockchain is seen as an ideal solution for identity management, cases like Bitcoin highlight the importance of anonymity. Certain IoT devices, such as wearables and smart vehicles, may need to conceal private information. Protecting these devices requires the integration of encryption technologies, which must consider the devices' limited resources and cost constraints.

Traceability: Blockchain's traceability is characterized by its ability to maintain a complete and unalterable history of data from its origin. Every transaction is transparently and chronologically recorded in consecutive blocks, allowing stakeholders to trace the actions that led to the creation of the data. This ensures full visibility of the data's lifecycle, reinforcing trust by guaranteeing the transparency, authenticity, and verifiability of all information recorded on the blockchain.

Reliability: The reliability of blockchain stems from its robust structure, built on decentralization and consensus mechanisms such as Proof-of-Work (PoW) or Proof-of-Stake (PoS). Decentralization mitigates the risk of single points of failure, as every node maintains a copy of the ledger, ensuring resilience. Consensus mechanisms ensure agreement on the ledger's state, boosting confidence in the data's accuracy. Combined with the immutability provided by cryptography, this architecture forms a reliable foundation for a variety of applications by safeguarding the blockchain's integrity against tampering or failure.

3) Consensus Algorithms

The consensus algorithm is at the heart of blockchain technology, ensuring the integrity and security of the blockchain network. It is a protocol by which the nodes of the blockchain network reach unanimous agreement on the current state of ledger records. Different blockchain platforms use different algorithms to reach consensus, and each algorithm works and executes differently.

The principle of these algorithms can be presented as follows [69], [70], [71]:

Proof of Work (PoW): PoW is a foundational consensus mechanism in blockchain. It determines which miner will have the privilege to create the next block in the chain. This process requires miners to solve a complex cryptographic puzzle, which serves as a security guarantee. The first node to solve this mathematical challenge is rewarded with the opportunity to forge the next block. PoW demands significant computational power, making the process highly competitive and contributing to the network's security and robustness. PoW gained prominence through Bitcoin, where it ensures the blockchain's security and integrity by incentivizing miners to invest considerable resources in block creation. However, despite its proven effectiveness, PoW faces criticism for its substantial energy consumption, raising environmental concerns.

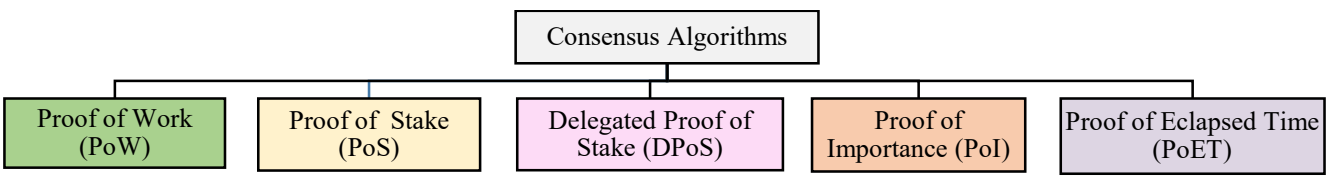

Fig3: The principle of Consensus Algorithms

Proof of Stake (PoS): PoS represents a novel approach to blockchain consensus, differing from traditional Proof of Work. In PoS, validators participate by staking a portion of their cryptocurrency, with their economic stake reflecting their importance in the network. Validators are selected based on their financial commitment to create new blocks, eliminating the need for energy-intensive mining. PoS provides a more energy-efficient alternative while maintaining security by aligning validators' interests with the network's well-being. This approach offers a sustainable and cost-effective solution as blockchain technology continues to evolve.

Delegated Proof of Stake (DPoS): DPoS is an advanced evolution of PoS, introducing democratic governance into blockchain technology. Participants can vote for delegates responsible for validating new blocks, promoting decentralization and community engagement. Token holders can stake their tokens to support preferred delegates, adding an economic dimension to participation. DPoS creates a more transparent and interactive blockchain ecosystem, providing financial incentives to participants. By integrating voting, delegation, and reward mechanisms, DPoS aims to build a dynamic and secure blockchain infrastructure that aligns the interests of users with the network's overall efficiency and security.

Proof of Importance (PoI): PoI is an innovative consensus algorithm designed to evaluate the significance of individual nodes within a cryptocurrency system, particularly in block generation. Unlike traditional methods like PoW and PoS, PoI considers factors such as transaction history, reputation, and overall network activity to assess the importance of a node. This encourages active and responsible participation, improving network performance. Priority in block creation is granted to the most important nodes, fostering efficiency and fair distribution of responsibilities. PoI addresses some of the limitations of traditional consensus mechanisms, offering a dynamic approach that enhances scalability and overall efficiency while encouraging meaningful participation from network participants.

Proof of Elapsed Time (PoET): PoET is a consensus algorithm that emphasizes fairness in block creation, particularly in systems where user authentication is critical. In PoET, each validator on the network has an equal opportunity to produce a block. Validators generate a random delay value, and the validator with the shortest delay is selected to add their block to the chain. This ensures fairness by eliminating any advantage or privilege, as selection is based purely on chance. PoET's reliance on secure randomization and the absence of resource-intensive computations make it an energy-efficient alternative to traditional mechanisms like PoW. It enhances the scalability and sustainability of blockchain networks while preserving a high level of security and decentralization.

4) Blockchain types

Blockchain technology is applied in various domains. From an access perspective, there are four types of blockchain [63], [64], [66], [67], [69], [70] : public, private , consortium and hybrid , each catering to specific purposes and applications.

Public Blockchain: Public blockchain function without a centralized authority, relying on numerous participating nodes but offering a relatively lower level of trust compared to private systems. Commonly used in sectors like the IoT, public blockchain are decentralized and scalable. However, they face challenges such as low throughput, high energy consumption, significant latency, and high computational power requirements. Additionally, they are vulnerable to a 51% attack, which could compromise the integrity of the system.

Private Blockchain: Also known as an "authorized blockchain" or "private distributed ledger," private blockchain are governed by a single entity that has full control over the network. Access to the network is restricted, with different levels of authorization for participating nodes. Private blockchain typically use consensus mechanisms like "proof of authority" or "proof of stake" to achieve consensus quickly and address byzantine faults. Despite these advantages, private blockchain can become complex, especially when managing networks with a large number of nodes.

Consortium Blockchain: A consortium blockchain is a variant of the private blockchain but with decentralized governance. Instead of being controlled by a single entity, governance is distributed among a group of selected participants, fostering transparency, accountability, and collaboration. This type of blockchain is ideal for industries where data confidentiality and regulatory compliance are critical, such as supply chain management, finance, and healthcare. Consortium blockchain offer a balance between the advantages of decentralization and the need for a controlled environment, making them suitable for collaborative projects.

Hybrid Blockchain: Hybrid blockchain combine the strengths of both public and private blockchain, offering flexibility and adaptability. By merging the access control capabilities of private blockchain with the security and transparency of public blockchain, hybrid blockchain allow for selective partitioning of data. Sensitive information remains private within a closed network, while other data can be made publicly accessible.

.

TABLE I
COMPARISON OF BLOCKCHAIN TYPES

Features	Public Blockchain	Private Blockchain	Consortium Blockchain	Hybrid Blockchain
Architecture	Decentralized	Partially Decentralized	Partially Decentralized	Hybrid (Mix)
Security Level	Lowest trust	High	Moderate	High
Permission	Permission less	Permissioned	Permissioned	Selectively
Traceability	Transparent	Controlled	Controlled	Controlled /Selective
Flexibility	Limited	High	Moderate	High
Speed	Moderate	High	Moderate	Moderate
Efficiency	Moderate	High	Moderate	Moderate
Immutability	High	High	Moderate	High (Selective)

This makes hybrid blockchain highly versatile, well-suited for applications like supply chain management and finance, where specific requirements for confidentiality and transparency must be met. Hybrid blockchain provide a practical solution, enabling organizations to customize their blockchain implementations to meet unique needs while staying adaptable to future technological developments.
The table I compares the different types of blockchain

B. Blockchain-IoT applications

1) Raisons of integrate blockchain in IoT

Integrating blockchain into the IoT offers numerous advantages and opportunities. Below are the key reasons why blockchain is viewed as a promising technology for IoT [61], [63], [64], [69],[72]:

Security and Privacy: Blockchain provides strong protection for IoT data through advanced cryptographic techniques, ensuring that data cannot be tampered with or accessed without authorization. This ensures the confidentiality of sensitive information, making blockchain particularly valuable for secure IoT environments.

Traceability and Immutability: Blockchain guarantees traceability by recording all transactions in an immutable ledger. This ensures the integrity of the data generated by IoT devices. Traceability is especially critical in sectors like supply chain management, where being able to track goods and processes accurately is essential.

Identity and Authorization Management: Blockchain simplifies the management of identities and authorizations for IoT devices. Each device can be assigned a unique identity and permissions, increasing the overall security of the IoT network by ensuring that only authorized devices can perform specific actions.

Reduced Fraud and Errors: Blockchain makes it significantly harder to falsify data or introduce errors when managing information related to IoT devices. This capability is particularly beneficial in fields such as environmental monitoring, energy management, and real-time data collection, where accurate and reliable data is crucial.

Cost Reduction: Blockchain has the potential to reduce costs associated with IoT systems by automating essential processes like billing, data management, and contract execution. By enhancing operational efficiency, blockchain can contribute to significant cost savings across various IoT applications.

Transaction Automation: Blockchain leverages smart contracts to automate transactions in IoT ecosystems. Smart contracts execute automatically when predefined conditions are met, for example, triggering an IoT sensor or activating a system based on specific environmental criteria. This automation streamlines operations and reduces the need for manual intervention.

2) Applications areas

The integration of blockchain technology into IoT applications represents a crucial development in the sector (see Figure 4). With IoT applications growing in number and significance daily, they are now reaping the benefits of blockchain's unique attributes. From everyday consumers to major industries, IoT has firmly established itself as a driving force in the quest for a smarter, more interconnected world [66]. Looking into the future, it is becoming increasingly clear that the introduction of blockchain into the IoT ecosystem is not just a trend but a transformative step forward. The convergence of these two technologies is extremely promising, leveraging blockchain's pillars of decentralization, security, and transparency to fortify the foundations of the IoT. Smart home systems, smart grids, smart healthcare solutions, and a whole host of innovative smart accessories are embracing this paradigm shift [61], [62], [63], [64], [65], [66], [67], [68], [69].

Figure 4 present some applications areas of blockchain technology in IoT environments:

In this part, we delve into a comprehensive exploration of how integration with blockchain is reshaping IoT applications in various areas, paving the way for increased security, trust, and efficiency in IoT environments.

Smart Cities [61], [64], [67]: The integration of blockchain technology into smart cities is revolutionizing urban development by implementing intelligent infrastructure, such as smart lighting, water management, and parking systems. This integration not only strengthens data security and transparency, ensuring the integrity of information and preventing unauthorized access, but also supports transparent urban governance through secure digital identity verification and transactions. Blockchain in smart cities promotes sustainable urban development, enhances citizen services, and contributes to a more resilient urban environment, ultimately shaping the future of interconnected cities.

Smart Home and Appliances [61], [62], [67]: In the realm of consumer IoT devices, blockchain enhances the security and functionality of smart homes and appliances. With utilities like smart voice assistants (Siri, Alexa, and Google Assistant) and an array of devices (smart fans, TVs, lighting systems, refrigerators, and wearables), blockchain ensures data privacy and integrity, protecting against unauthorized access and tampering. It also enables secure and transparent transactions, fostering trust and user-friendly experiences. This integration marks a significant leap toward safer, more connected, and efficient smart homes, empowering consumers to manage their daily activities with greater control and security.

Smart Healthcare [61], [64], [65], [67],[73], [74] : In smart healthcare systems, blockchain plays a pivotal role in enhancing data security and automating processes like insurance claims and billing via smart contracts. This innovation empowers patients, granting them control over their health data and enabling more active participation in healthcare decisions. Blockchain also expands healthcare accessibility to remote areas lacking physical infrastructure. By combining IoT and blockchain, the integration bridges healthcare disparities, promotes patient-centric care, and delivers secure, efficient healthcare services.

Smart Industries [65], [67]: Blockchain integration within smart industries brings a transformative leap to industrial processes. IoT has already advanced these sectors through innovations like smart sensors, advanced control systems, and autonomous robots. Blockchain adds a crucial layer of security and transparency, ensuring data integrity and protecting against unauthorized access. This integration enables transparent supply chain management, enhancing reliability, efficiency, and collaboration within industries and driving them toward smarter, more productive futures.

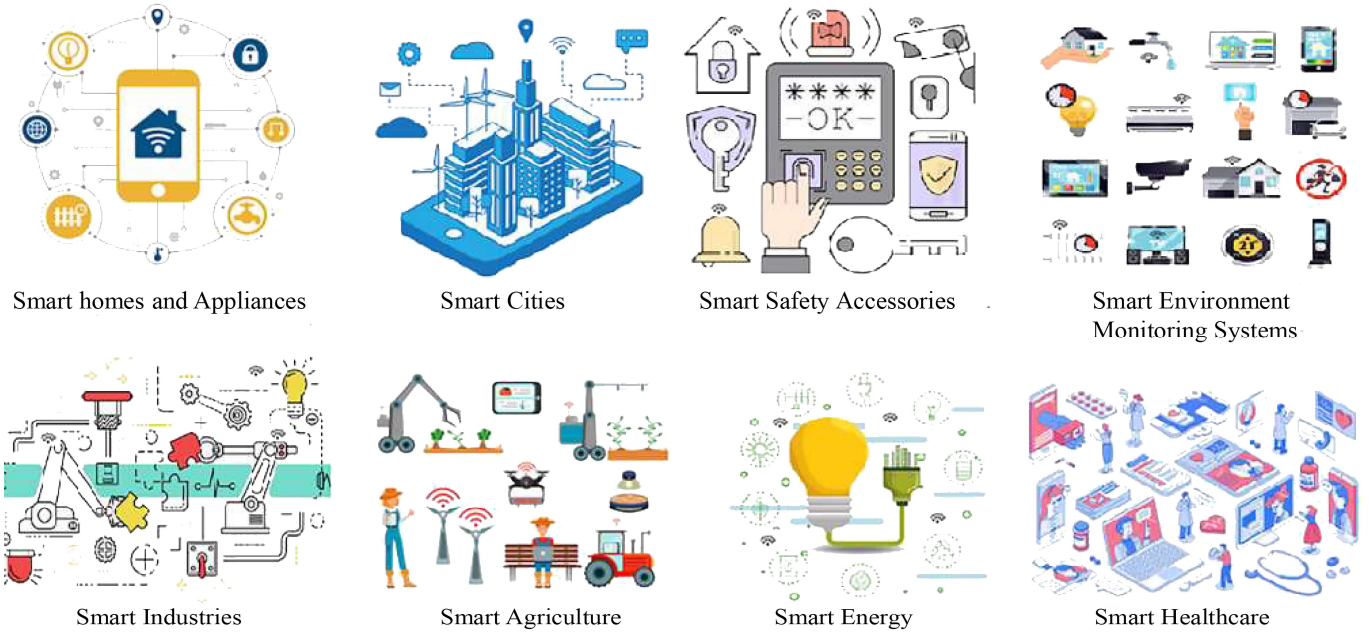

Fig 4: applications areas of blockchain technology in IoT environments.

Smart Agriculture [61], [65], [67] : The integration of blockchain and IoT is revolutionizing smart agriculture by optimizing resource use and improving crop quality. IoT enables real-time data collection on factors such as soil moisture and weather conditions, while blockchain ensures data integrity and protects against unauthorized access. This integration enhances product traceability, promotes trust in the supply chain, and streamlines transactions via smart contracts. It also fosters sustainability, efficiency, and trustworthiness, benefiting both stakeholders and consumers.

Smart Energy [64], [65]: Blockchain is being integrated into smart energy systems, enhancing traditional power grids through IoT's real-time communication and sensing capabilities. These technologies monitor electricity generation, consumption, and transmission lines, improving overall efficiency. Blockchain ensures the security and transparency of energy data, allowing only authorized access and supporting peer-to-peer energy trading. This decentralized approach to energy management promotes sustainable, reliable, and environmentally conscious solutions.

Smart Environment Monitoring Systems [65], [66]: Combining blockchain with IoT in smart environment monitoring systems enhances the monitoring and protection of natural resources. IoT sensors collect real-time data on critical environmental factors such as temperature, air quality, and soil health. Blockchain ensures the security and integrity of this data, providing reliable insights for ecological decision-making. This integration helps tackle environmental challenges by offering transparent, accurate, and secure data to support sustainable environmental management practices.

Smart Safety Accessories [66]: Blockchain's integration into smart safety accessories, such as video surveillance cameras, biometric systems, and geolocation solutions, enhances security in various aspects of human life. It also extends to industrial and military IoT applications, including surveillance robots and wearable biometric equipment. Blockchain guarantees the integrity of security-related data through decentralized ledgers, ensuring transparency and trustworthiness in data handling. This enhances safety and security in various environments, from everyday settings to high-stakes industrial and military applications.

3) Integration of Blockchain technology in IoT

Integrating blockchain technology into an IoT ecosystem is a strategic process that leverages the unique attributes of blockchain, such as decentralization, security, and transparency, to enhance the functionality and security of IoT devices and the data they generate. This integration involves a series of well-defined steps aimed at maximizing the potential benefits [66], [68], [75] :

Figure 5 below summarizes the integration of blockchain technology in the IoT environment:

Step1 (Defining Use Cases): The first phase involves identifying specific use cases within the IoT ecosystem where blockchain technology can deliver added value. Key areas include supply chain management, asset tracking, and data source verification, among others.

Step2 (Selecting Suitable Blockchain Platforms): Based on the identified use cases, selecting an appropriate blockchain platform is crucial. Public, private, and consortium blockchain each have distinct advantages and limitations, and the choice should align with the specific requirements of the IoT application.

Step 3 (Designing System Architectures): Developing a robust system architecture is essential for the successfully integration blockchain and IoT. This involves creating a framework that ensures seamless communication between IoT devices and the blockchain network.

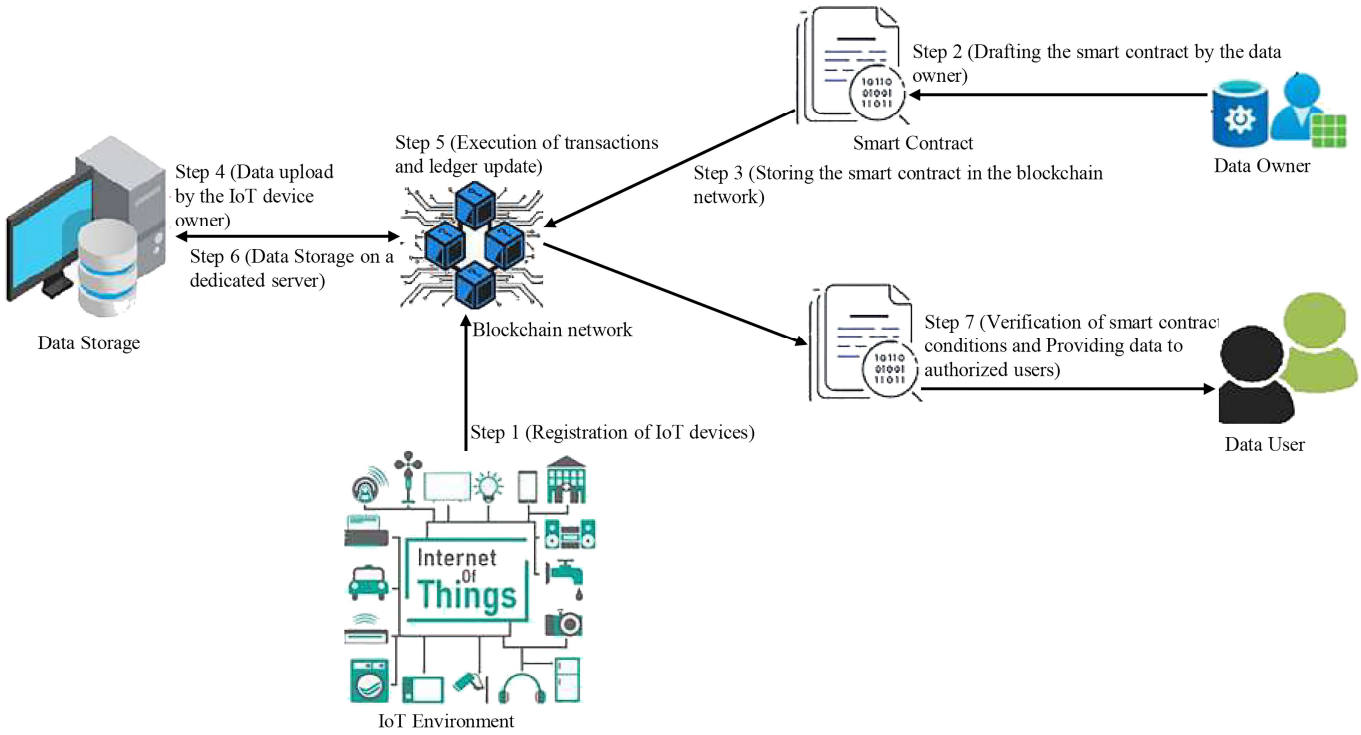

Fig 5: Integration of blockchain and IoT based system

Step 4 (Ensuring Data Security and Privacy): IoT generates vast amounts of sensitive data. Blockchain can enhance data security by encrypting and securing the information. Moreover, privacy considerations like data anonymization must be addressed to comply with regulations such as the General Data Protection Regulation (GDPR).

Step 5 (Implementing Smart Contracts): Smart contracts, which are self-executing codes stored on the blockchain, can automate various processes in the IoT ecosystem. These contracts trigger actions when predefined conditions are met, facilitating efficient and autonomous operations.

Step 6 (Establishing Device Identity Management): Managing the identity of IoT devices is critical to preventing unauthorized access and maintaining network integrity. Blockchain offers a secure mechanism for managing device identities.

Step 7 (Data Validation): Ensuring the accuracy and integrity of IoT data is crucial. Blockchain's immutable ledger can validate data generated by IoT devices, creating a trustworthy and tamper-proof record.

Step 8 (Compliance and Regulation): Adherence to legal and regulatory requirements is critical. Blockchain's transparency can aid regulatory compliance, and compliance should be an ongoing priority.

Step 9 (Monitoring and Maintenance): Continuous monitoring and maintenance of the integrated system are necessary to address any issues, ensure optimal performance, and adapt to evolving requirements.

The integration of blockchain into an IoT environment offers several advantages, including enhanced security, trust, and efficiency. It creates a tamper-proof and transparent record of IoT data, reducing the risk of data manipulation and fraud. Ultimately, this synergy between blockchain and IoT holds the potential to revolutionize various domains by providing a foundation for more secure and reliable IoT applications.

C. *The Internet of Things*

1) *Architecture*

The IoT concept revolves around creating a network that facilitates the effective management of information flow between various connected devices. In practice, this presents significant challenges due to the diversity of IoT devices, such as smart sensors and data centers, all of which demand seamless and secure communication [65]. Compatibility between all devices requires specialized communication protocols, standardized structures, application compatibility, advanced data processing capabilities, etc.

The fundamental operation of the IoT involves intelligent objects collecting data from physical sensors and transmitting it to data centers, either locally or in the cloud, or to other intelligent objects via gateways. The data received is processed to trigger various actions, adding complexity to applications such as autonomous cars. Although IoT applies to many domains and lacks standardization, a three-layer architecture model comprising the perception, network/transmission, and application layers is often adopted (as shown in Figure 6) to address scalability, interoperability, data distribution, computing power, and security considerations [66], [67], [76]. These three layers collectively enable a range of IoT applications, including those related to smart health, smart homes, smart cities, and other smart domains, by facilitating the implementation and delivery of data processing results via the application layer.

The application layer: situated just above the transmission layer in the IoT architecture, is a flexible and adaptable component that varies according to the specific implementation. This layer is responsible for analyzing and processing the data received from the underlying perception

and transmission layers, processing the information for various applications, and executing desired actions, such as controlling actuators. It serves as a bridge, transforming and transmitting data to other nodes or passing it on to other applications for further processing. Additionally, the application layer hosts user interfaces, enabling users to interact with the IoT system and perform actions, such as notifying a technician to service a piece of equipment. The functionality of this layer can vary considerably depending on the implementation, encompassing real-time monitoring, information digitization, data analysis, and hardware control, depending on the needs of the desired application. Within the application layer, five distinct protocols are presented[77] : MQTT, CoAP, REST, XMPP, and AMQP. Table II provides a brief description and characteristics of these protocol.

.

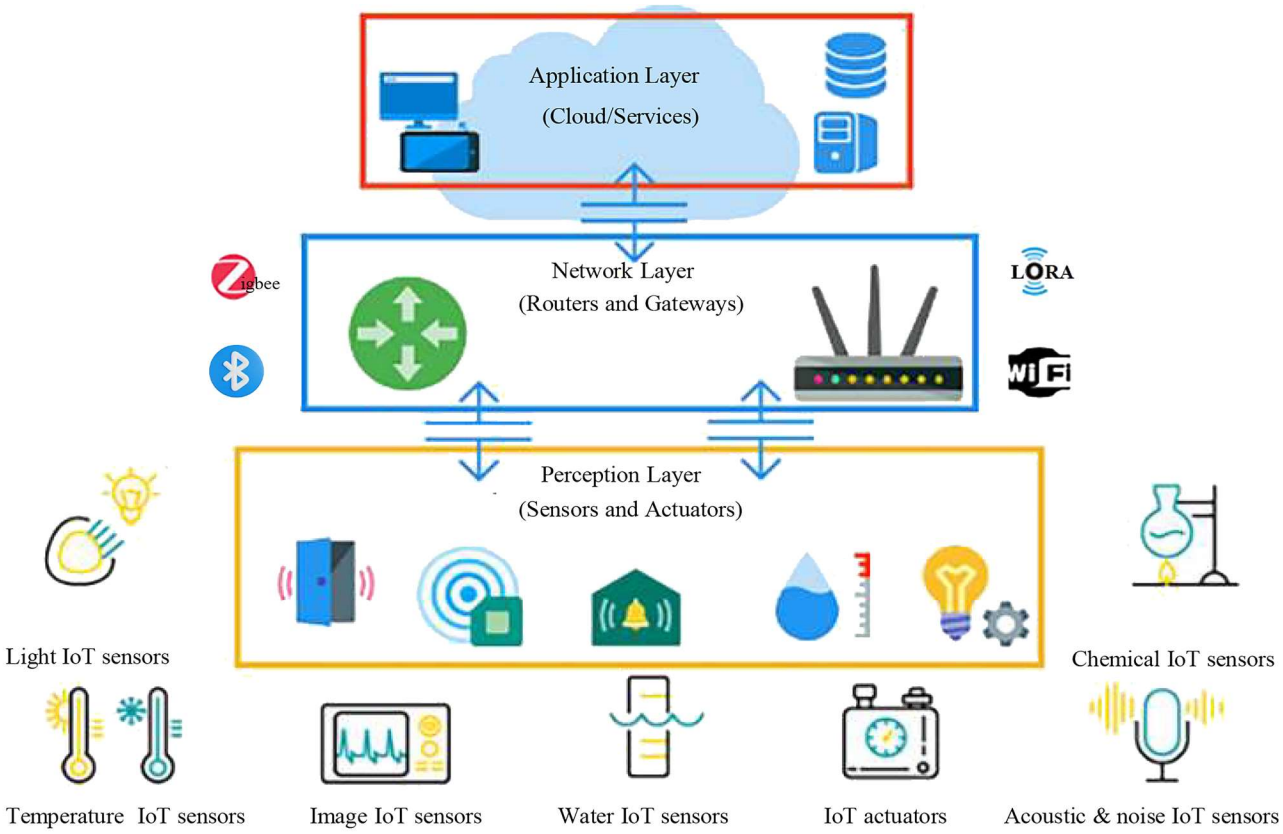

Fig 6: Generic architecture of IoT system.

TABLE II
DESCRIPTION AND CHARACTERISTICS OF PHYSICAL LAYER PROTOCOLS

Protocols	Description	Characteristics
MQTT	Message Queuing Telemetry Transport is a messaging protocol designed for publishing and subscribing messages. Ideal for IoT and limited resources. Requires particular attention to security.	Open nature, lightweight design, runs on TCP/IP, requires security measures.
CoAP	Constrained Application Protocol is a lightweight web transfer protocol for resource-constrained nodes and networks, suitable for machine-to-machine (M2M) applications. Requires Datagram Transport Layer Security (DTLS) for security.	Seamless integration with HTTP, suitable for IoT, security via DTLS.
REST	Representational state transfer is a versatile architectural style for distributed hypermedia systems and web applications. It is based on principles such as client-server separation, statelessness, caching, uniform interface and layered architecture.	statelessness for enhanced visibility and scalability, caching for improved network efficiency, a uniform interface ensuring consistency, layered system architecture for flexibility and scalability and dynamic code capability.
XMPP	Extensible Messaging and Presence Protocol is an open XML protocol essential for real-time communication, suitable for instant messaging and presence management. May present security risks.	Real-time communication, scalability, suitable for IoT, requires security measures.
AMQP	The Advanced Message Queuing Protocol is an essential open standard for business messaging, guaranteeing asynchronous communication between organizations and platforms. Focused on security, reliability a	security ,reliability, interoperability, ISO and IEC international standards, multi-layer structure.

TABLE III
DESCRIPTION AND CHARACTERISTICS OF NETWORK LAYER PROTOCOLS

Protocols	Description	Characteristics
WiFi	WiFi, an abbreviation for Wireless Fidelity, is a ubiquitous and widely recognized wireless communication technology based on the IEEE 802.11 standard.	Continuous improvements, increased safety, coverage of around 100 meters, versatility.
Bluetooth	Bluetooth Low Energy (BLE), also known as Bluetooth Smart, is a preferred choice for IoT implementations because of its focus on ultra-low power consumption, making it ideal for low-power applications.	Low energy consumption, scalability, positioning services, compatibility.
LoRaWAN	Long Range Wide Area Network is a crucial LPWA (Low Power, Wide Area) protocol essential for the IoT, with low power consumption and bidirectional communication.	Low power consumption, long-range communication, enhanced security
ZigBee	related to Bluetooth Low Energy (BLE) is a emerging IoT protocol with a robust security structure, adapted to limited resources	Enhanced security, low energy consumption, short-distance communication (up to 200 meters) , adaptability.
Z-Wave	Wireless communication protocol operating on an exclusive frequency band.	Low power consumption , frequency isolation, interference reduction .

Network or Transmission Layer: In the IoT architecture, the transmission or network layer, situated between the perception and application layers, plays a crucial role in facilitating the flow of data within the Internet of Things ecosystem. At this layer, data collected by smart sensors is transformed and transmitted to the application layer through various communication channels and protocols, enabling it to be processed, analyzed, aggregated, and encoded. In addition to basic packet routing, this layer also manages network functionality. IoT implementations mainly prefer wireless protocols for their flexibility, enabling deployment in remote or difficult environments and easy node management. In contrast, wired sensor networks are preferred in scenarios where reliability and speed of data transmission are essential, such as in healthcare. Intelligent IoT sensors are essential for seamless communication, interaction with the physical world, and the prevention of data conflicts. The transmission layer serves as a vital conduit, connecting devices and enabling the transformative potential of IoT in diverse applications. In the network layer, we introduce five distinct network protocols that address the application layer[77]: WiFi, Bluetooth, LoRaWAN, ZigBee, and Z-Wave. Table III provides a brief description and characteristics of these protocols.

Physical or Perception Layer: In the IoT, the perception or physical layer serves as the critical interface between the tangible, real world and the digital world and is the cornerstone of this transformative technology. It includes a wide range of physical devices that play a central role in the IoT ecosystem, including sensors such as those that measure temperature, humidity, and light, actuators with electrical, mechanical, or hydraulic capabilities, video trackers such as IP cameras, and essentially any device capable of interacting with others via the exchange of data. What really sets the intelligent sensors in this layer apart is their integration of microprocessors, which enable them not only to collect data but also to process it. This additional intelligence enables essential functions such as data normalization, noise filtering, and data transformation, all of which are crucial for refining the information collected before transmitting it to other devices on the network. In this way, this perception layer bridges the physical and digital worlds, laying the foundation for IoT's transformative potential.

For the physical layer, the IEEE 802.15.4 protocol is a fundamental wireless communications standard, primarily designed for this layer in the Internet of Things architecture. It specializes in facilitating low-cost communications over short distances and provides a solid foundation for low-speed, short-range wireless networks [77].

2) Characteristics

The IoT offers many benefits due to its unique characteristics [67], including:

Interconnectivity of heterogeneous systems: IoT networks enable communication between various devices and hardware platforms, facilitating the interaction between different networks.

High scalability: IoT systems are capable of establishing connections between all entities through a universal information and communication system, ensuring widespread integration.

Security considerations: These include physical security, data protection, and the increasing interconnection of systems equipped with IoT devices via intranets and the internet, addressing potential vulnerabilities.

Seamless connectivity: IoT ensures access to information anytime and anywhere, contingent on proper authorization and authentication of stakeholders.

Dynamic change: IoT devices exhibit a constantly evolving state, whether they are asleep, awake, connected, disconnected, in a particular location, or moving at various speeds.

Connected object services: IoT contributes to privacy protection and maintains semantic consistency regarding device-related constraints, thanks to advances in technologies that bridge the physical and digital worlds.

IV. SURVEY METHODOLOGY

In this survey, our focus was on specific scientific databases, as their extensive collection of articles and conference proceedings significantly enhances comprehensive data exploration. The databases included in our survey are:

- ScienceDirect;
- MDPI;
- IEEE Explore;
- Wiley/Hindawi;
- Springer.

A. Search Strategy

There are a multitude of publications concerning blockchain technology and its implementation in the IoT environment. This is why we used specific keywords when searching the designated digital libraries in order to acquire primary studies in relation to the research context. These criteria are essential for finding the most relevant and up-to-date resources for our research. The libraries were also chosen for their user-friendliness and simplicity. Consequently, we used the following keywords to search each of the online digital libraries: ((“Blockchain” OR “Blockchain Technology”) AND (“Internet of Things “OR “IoT”) AND (“Smart Home” OR” Smart City” OR “Healthcare” OR “Industrial IoT” OR “Smart Agriculture” OR “Smart Energy”) AND (“Security” OR “Privacy”) . To ensure that our study reflected current academic insights, we focused on publications from 2021 to 2023.

B. Eligibility Criteria

The goal of this study is to provide a comprehensive overview and assessment of the applications and uses of blockchain technology within IoT. To achieve this, we applied inclusion and exclusion criteria to filter out irrelevant articles. The inclusion criteria focused on the article’s relevance to blockchain technology and its application in IoT across various domains. Eligible articles needed to be written in English, peer-reviewed, and published between 2021 and 2023. In contrast, the exclusion criteria targeted articles that were not directly related to blockchain technology’s implementation in IoT, were not peer-reviewed, or were unpublished literature in English.

.

C. Selection Results

The selection process for this study was carried out in two distinct phases. In the first phase, we evaluated the titles and abstracts of all the studies gathered. We conducted a broad search that initially identified over 100 studies using the specified keywords. The pool was then reduced from more than 100 to 73 articles by applying the inclusion and exclusion criteria to the titles and abstracts. In the second phase, we conducted a thorough review of the full texts. After applying the criteria to the remaining 73 articles, an additional 13 were excluded. Ultimately, our survey included 60 primary studies, covering six application domains: smart home, smart city, healthcare, industrial IoT, smart agriculture, and smart energy.

V. RESULTS AND DISCUSSION

In this section, we present various studies that have investigated the integration of blockchain technology within the IoT environment. We provide an in-depth analysis of the key characteristics of each included article, such as their primary information, objectives, methodologies employed, benefits, and limitations.

Based on the data illustrated in Figure 7, it is evident that 16.66% of the total articles were published in 2021, 40% in 2022, and 43.33% in 2023. Additionally, Figure 8 shows that 32% of the articles were sourced from the Science Direct database, 25% from IEEE, 23% from MDPI, 13% from Wiley/Hindawi, and 7% from Springer.

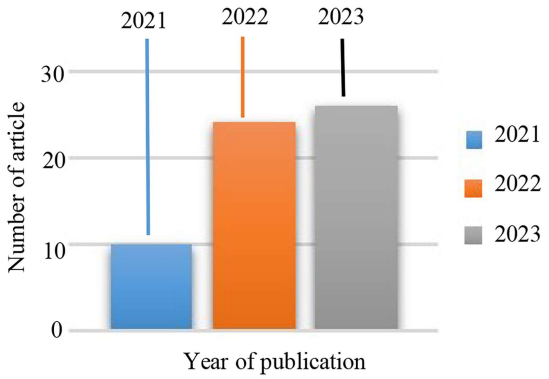

Fig 7: Article by year of publication.

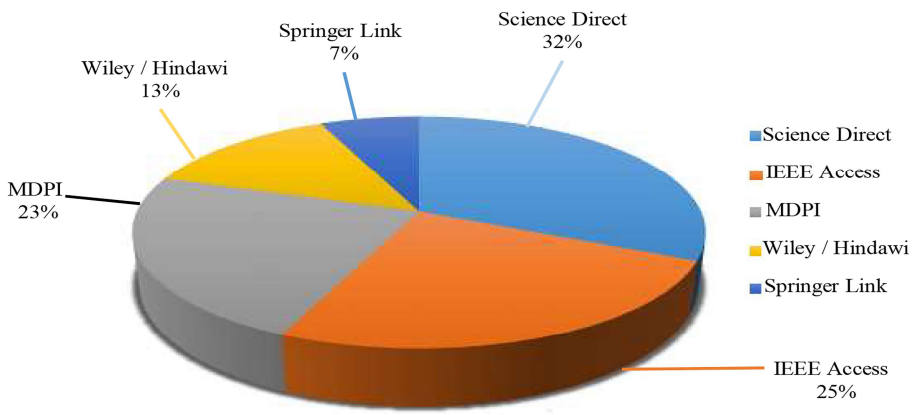

Fig 8: publications according to scientific database.

It should be noted that research into the implementation of blockchain technology in IoT environments is considered innovative and will require further development and testing in a variety of IoT environments. Additionally, the implementation of systems integrating blockchain technology in IoT environments presents challenges and takes longer than standard architectures. This explains why blockchain-based approaches are not yet widespread in some research domains. Nevertheless, many approaches that integrate blockchain technology with IoT in their designs are showing promising results. The following results provide an overview of the objectives, methodologies employed, advantages, and disadvantages of previous research concerning the implementation of blockchain technology in the Internet of Things (IoT) environment in various domains, including smart home, smart city, healthcare, industrial IoT, smart agriculture, and smart energ

.

A. Blockchain for smart homes IoT systems

In the context of enhancing security, privacy, and overall functionality within smart homes, numerous studies have investigated the application of blockchain technology in IoT environments. Table IV presents a comprehensive overview of the objectives, methodologies, benefits, and limitations of these past research efforts, shedding light on the potential and challenges of blockchain integration in smart home systems

TABLE IV
STUDIES CARRIED OUT ON SMART-HOME BASED ON BLOCKCHAIN TECHNOLOGY.

References	Objectives	Used Methods	Benefits	Limitations
[1]	Enhance security in smart home communication networks by combining blockchain-based secure communication and machine learning techniques.	-Blockchain for secure communication and ledger generation. -Applying a cloud-based data evaluation layer. -Employing a neural network for training and classification. -Implementing the dragonfly algorithm for data selection.	-Enhanced security through blockchain-based authentication. -Reduced computation complexity. -High prediction accuracy for identifying false authentications.	-Scalability and energy consumption issues.
[2]	To enhance security and privacy in smart home networks by utilizing a combination of Blockchain technology and a Hybrid Deep Learning (HDL) model.	-Integration of BC technology for data confidentiality and network security. -Employment of HDL model for malicious activity detection. -Use of Gradient Based Optimizer (GBO) for hyper-parameter tuning. -Data preprocessing for standardization.	-High accuracy in detecting malicious activities -Enhanced security and privacy.	-Complexity in implementing Blockchain technology and HDL technologies
[3]	Propose a lightweight authentication mechanism and request queue management for mitigating Distributed-Denial-of-Service (DDoS) attacks in smart home networks using blockchain technology.	-Utilizing Ethereum blockchain and smart contracts for decentralized authentication and ledger system. -Employing a single server queuing system model to manage DDoS attacks.	-Lightweight and efficient authentication mechanism. -Low computational costs. -Resilience to DDoS attacks.	-Gateway reliability issues.
[4]	Develop a private blockchain-based smart home network architecture empowered with a Fused Real-Time Sequential Deep Extreme Learning Machine (RTS-DELM) system model for intrusion detection and prevention.	-Use of a private blockchain network. -Implementation of RTS-DELM for intrusion detection. -Application of data fusion techniques for improved accuracy.	-Enhanced security and privacy in smart home networks. -Real-time data analysis. -High accuracy in intrusion detection	-Lack of recovery after attacks.(Focuses on prevention but not on recovery from attacks.)
[5]	Design a blockchain-based edge computing method to secure smart home systems, provide energy usage prediction, and user profiling.	-Integration of IoT, energy data, and machine learning. -Blockchain technology for data security. -Use of ARIMA and LSTM models for energy usage prediction. -Edge computing for local data processing.	-Enhanced security and data privacy -Real-time monitoring and notifications. -Transparency and immutability of data. -Accurate energy usage prediction	-Scalability issues -Initial setup costs and technical requirements.
[6]	Enhance security and privacy in smart homes by replacing centralized systems with a consortium blockchain and Inter-Planetary File System (IPFS).	-Free certificate less aggregated signature (CLAS) scheme for message authentication. -Employ Merkle root hash verification for data integrity audit. -Use consortium blockchain and IPFS for data storage and management.	-Increased security and privacy. -Reduced computational and communication overhead for devices. -Enhanced data integrity -Automated audit	-Communication overhead. -Complexities in implementing blockchain and IPFS

[7]	Develop an architecture aimed at ensuring data integrity and strong security while preserving the validity of blockchain transactions.	-Explore four different consensus algorithms -Transactions (CHT), Merkle Hash Tree (MHT), Odd and Even Modified Merkle Hash Tree, Modified Merkle Hash Tree (MMHT). -Use a smart contracts for network efficiency.	-Enhance data security and integrity. -Efficient execution time of the MMHT consensus algorithm.	-Complex relationship between transactions, consensus algorithms, and hash functions.
[8]	Develop a secure smart home system using blockchain and cloud services for data access control and management.	-Utilize various cloud service combinations for smart home control core. -Combine blockchain and password technology for secure data access control. - Extend the attribute-based access control model (ABAC) for fine-grained access control.	- Enhanced security. - Fine-grained access control. - Anonymity and privacy protection. - Scalability for dynamic authorization.	- Increased communication and computational load.
[9]	Enhance the security of smart home networks by implementing a low-end design using private blockchain technology and localization.	-Implement localization via Received Signal Strength Indicator (RSSI) based trilateration to identify the source of attacks. -Incorporate Kalman filter for enhanced accuracy. -Private blockchain technology for device recognition and access control.	-Better performance (Private blockchain). -Improved security for home networks.	-Require additional hardware and software components.
[10]	Develop a privacy-preserving mechanism for smart homes using blockchain technology and attribute-based access control.	-Combining attribute-based access control with smart contracts and edge computing. -Implementing Register and Access contracts. -Integrating differential privacy for data aggregation.	-Enhanced security and privacy for IoT devices. -Resilience against attacks. -Scalability with edge computing. -Integration of differential privacy. -Fine-grained access control.	-Complexity in managing attributes.

After analyzing the data presented in Table IV, it is evident that the articles [1]-[10] collectively delve into the integration of blockchain technology into smart home IoT systems, aiming to enhance security and privacy while addressing various challenges and improving functionalities. The integration of blockchain technology in smart home environments seeks to fortify these systems against emerging threats and vulnerabilities. [1] Enhances security through blockchain-based secure communication and machine learning techniques. It employs blockchain for secure communication, cloud-based data evaluation, neural network training, and the dragonfly algorithm for data selection. Benefits include enhanced security through authentication and high prediction accuracy. Challenges involve scalability and energy consumption issues. [2] Focuses on enhancing security and privacy using blockchain technology and Hybrid Deep Learning (HDL) models. Methods integrate blockchain for data confidentiality and HDL for malicious activity detection, leveraging Gradient-Based Optimizer for tuning. It aims for high accuracy in detecting malicious activities but faces complexity in implementation and technology integration. [3] Proposes a lightweight authentication mechanism using Ethereum blockchain and smart contracts to mitigate DDoS attacks. It offers decentralized authentication with low computational costs and resilience against DDoS attacks. However, reliability issues with gateway nodes are significant limitations. [4] Develops a private blockchain-based smart home network architecture for intrusion detection and prevention using Real-Time Sequential Deep Extreme Learning Machines (RTS-DELM). It ensures enhanced security and privacy with real-time data analysis but lacks recovery mechanisms post-attacks. [5] Designs a blockchain-based edge computing method integrating IoT, machine learning, and blockchain for enhanced security and data privacy. It enables real-time monitoring, data immutability, and accurate energy usage prediction. Challenges include scalability issues and initial setup costs. [6] Enhances security and privacy in smart homes through a consortium blockchain and Inter-Planetary File System (IPFS). It employs a certificate less aggregated signature scheme and Merkle root hash verification for enhanced data integrity and reduced overhead. Challenges involve communication overhead and implementation complexities. [7] Focuses on data integrity and security using different consensus algorithms and smart contracts. It aims to improve efficiency with the MMHT consensus algorithm but faces challenges in managing transaction relationships and hash functions. [8] Develops a secure smart home system using blockchain and cloud services for fine-grained access control. It enhances security, anonymity, and scalability for dynamic authorization but increases communication and computational load. [9] Enhances smart home network security through private blockchain technology and localization via RSSI. It improves performance but requires additional hardware and software components, limiting scalability. [10] Implements privacy-preserving mechanisms using blockchain and attribute-based access control. It integrates smart contracts, edge computing, and differential privacy for enhanced security and scalability.

Challenges include managing attributes and initial setup complexities.

Analyzing the various studies [1]-[10], it becomes evident that integrating blockchain into smart home IoT systems addresses critical challenges related to security, privacy, scalability, and data management. However, it is essential to systematically examine how these technologies interact and complement each other to develop more robust, efficient, and adaptable smart home environments. By exploring the synergistic effects of combining advanced techniques such as decentralized authentication, edge computing, and distributed storage, we can better understand the potential of these integrated solutions to overcome existing limitations and enhance the overall functionality of smart home systems. In terms of **security and privacy**, approaches combining blockchain with advanced machine learning techniques show great potential for enhancing data security and privacy [1], [2]. For instance, using neural networks and the dragonfly algorithm can enhance security through blockchain-based authentication. To strengthen these methods, developing more energy-efficient and resource-effective algorithms is crucial [5]. Addressing **authentication and resilience**, lightweight authentication mechanisms based on blockchain, although effective against DDoS attacks, need improvements in node reliability and post-attack recovery [3], [4]. Enhancing node reliability and integrating robust recovery solutions could significantly bolster the resilience of these mechanisms. Regarding **scalability and cost**, edge computing methods and real-time processing solutions offer notable benefits for monitoring and prediction [5], [9]. However, challenges related to scalability and initial costs must be addressed. Developing more scalable and economically viable solutions could support broader adoption [6], [7]. In the realm of **data management and integrity**, distributed storage systems like IPFS and various consensus algorithms contribute to improved data integrity [6], [7]. Simplifying integration processes and reducing communication overhead are crucial for optimizing these solutions and enhancing their practical applicability. When considering **access control and anonymity**, attribute-based access control and differential privacy solutions provide granular control and enhanced privacy protection [8],[10]. Simplifying attribute management and reducing initial setup complexity could make these approaches more practical and accessible.

In conclusion, to improve IoT systems in smart homes, it is vital to combine techniques that enhance security, privacy, and resource management. Integrated solutions, such as decentralized authentication mechanisms, edge computing approaches, and distributed storage systems, show significant potential [1], [5], [6]. Addressing challenges related to scalability, cost, and implementation complexity will enable the development of more robust, secure, and adaptable IoT systems for modern smart homes [7], [8], [10].

B. Blockchain for smart cities IoT systems:

As the smart city concept continues to expand, the role of blockchain technology within IoT ecosystems is becoming increasingly prominent. To capture the scope and effectiveness of this integration, Table V outlines the key descriptions, methodologies, benefits, and limitations identified in previous research. This comprehensive overview sheds light on the advancements and challenges associated with applying blockchain technology to smart city infrastructures.

TABLE V
STUDIES CARRIED OUT ON SMART-CITIES BASED ON BLOCKCHAIN TECHNOLOGY.

References	Objectives	Used Methods	Benefits	Limitations
[11]	Enhance security in smart cities using blockchain technology, big data analysis, artificial intelligence algorithms, and practical Byzantine Fault Tolerance (pBFT) consensus protocol.	-Architecture based on perception layer, data processing layer, and blockchain layer. -Docker for deployment. -PySpark for data processing and machine learning. -Linear regression for prediction. -pBFT consensus protocol.	-Real-time data processing and analysis. - High accuracy in prediction using linear regression. - Energy-efficient pBFT consensus. - Improved smart city resilience.	-Resource intensive. - Dependency on technology infrastructure.
[12]	System based on blockchain and IoT to monitor post-production business processes of electronic devices and manage waste in a transparent and secure manner.	-Blockchain Implementation. -Smart Contracts. -IPFS Integration.	-Transparency. -Data Security. -Immutability. -Efficiency. -Cost Analysis.	-Scalability. -Resource Intensive.
[13]	Develop a decentralized and scalable solution using blockchain technology for establishing a sustainable smart city network.	-Used the CoAP protocol for IoT communications. - The CoAP server from the LibCoAP library as a manageable hub. -Smart Contract: Three smart contracts implemented using Solidity and mappings. -Ethereum blockchain for scalability and security.	-Scalability. -Performance (times for device creation, sensor reading, and query processing).	-Complexity (encryption methods). -Dynamicity (Private blockchain).
[14]	Develop a privacy-protected Support Vector Machine (SVM) training scheme using blockchain technology for secure collection of IoT data.	-Homomorphic cryptosystem for secure polynomial multiplication and comparison. -Secure SVM model training algorithm .	- Reduce interactions in encrypted data. - Data privacy. - Data integrity.	- Complexity of implementation. - Potential computational overhead.

[16]	Develop a Continuous Delivery and Continuous Verifiability method for IoT data flows in edge–fog–cloud.	- Continuous Delivery (CD). - Continuous Verifiability (CV). - Extraction, Transformation, and Load mechanism. - Directed Acyclic Graph (DAG) construction. - Private blockchain and smart contracts.	- Parallel patterns reduce CD/CV impact.	- Overhead in real-time verifiability strategy. - Limited experimental evaluation.
[15]	Develop a secured platform to enhance trust in digital governance's interoperability and data exchange using blockchain and deep learning.	- Optimal blockchain approach with the bonobo optimization algorithm for data authentication. - Integration of a lightweight Feistel structure with optimal operations for privacy preservation. - Deep reinforcement learning (DRL) model for intrusion detection and prevention.	- Strengthens digital governance's security, reliability, and privacy aspects.	- Complexity of integrating.
[17]	Develop a smart waste management system using IoT, Low Power Wide Area Network (LPWAN) and blockchain technologies.	- Smart bins with IoT technology to monitor trash volume and position. - Use of LPWAN for long-range data transmission. -Implementation of blockchain for authentication and key management.	- Increased data availability. - System auditability and traceability.	- Dependency on technology infrastructure.
[18]	Digitalization strategy for smart city using blockchain technology.	- Information system based on blockchain technology.	-Improvement of urban services. - Reduction of energy and water consumption, carbon emissions, pollution, and waste management.	- Dependency on technological infrastructure. - Complexity of implementation and process changes.
[19]	Implementation of a smart city IoT system with IaaS cloud computing architecture and improved routing performance improvement at the IoT network level.	- Application of blockchain for security and decentralization. - Network simulation using NS3 simulator to analyze performance-deciding parameters in the IoT topology. - Implementation of smart city IoT network in IaaS architecture.	- Performance optimization - enhanced security and scalability. - Cost-effective.	- Virtual simulation.
[20]	Develop a security architecture based on authentication and authorization for constrained environments during collaborative tasks for municipal smart cities.	-Integration of SDIoT (Software-Defined Internet of Things), Multi-chain blockchain, and smart contracts. -Use Software-Defined Networking (SDN) for security of services during collaborations between heterogeneous networks in municipal smart cities.	-Decentralization and data reliability. -Enhance security of collaborative services. -Managing and controlling data flows.	

After a thorough analysis of the data presented in Table V, we conclude that the studies [11]-[20] collectively explore the integration of blockchain technology into smart city IoT systems to address various challenges and improve functionalities. The integration aims to enhance security, transparency, efficiency, and privacy within smart urban environments. [11] Focuses on enhancing security in smart cities through a blockchain-based architecture incorporating advanced consensus protocols and utilizing Docker for efficient deployment. It leverages PySpark for data processing and machine learning, enhancing real-time data processing capabilities and achieving high prediction accuracy. Challenges include resource intensiveness and dependencies on technology infrastructure. [12] Introduces a blockchain and IoT system to monitor post-production business processes of electronic devices and manage waste transparently and securely. It integrates smart contracts for automated governance and IPFS for decentralized storage, ensuring data security, transparency, and efficiency. Scalability remains a significant challenge due to resource-intensive operations. [13] Proposes a decentralized and scalable smart city network using the CoAP protocol for IoT communications and Ethereum blockchain for smart contract management. It aims to improve scalability and performance in smart city infrastructure. Challenges include encryption method complexities and maintaining dynamic blockchain networks. [14] Develops a privacy-protected Support Vector Machine (SVM) training scheme using blockchain technology. It employs a homomorphic cryptosystem for secure data processing, ensuring data privacy and integrity in IoT applications. However, the implementation complexity and potential computational overhead pose significant challenges.

[15] Focuses on developing a secure platform for digital governance in smart cities using blockchain and deep learning. It integrates optimal blockchain approaches and lightweight structures for data privacy and integrity. Challenges include the complexity of integration and the operational changes required for adoption. [16] Introduces Continuous Delivery (CD) and Continuous Verifiability (CV) mechanisms for IoT data flows in edge–fog–cloud environments using private blockchain and smart contracts. It enhances data verifiability and integrity but faces challenges in real-time verifiability strategies and limited experimental evaluations. [17] Implements a smart waste management system using IoT and blockchain technologies, leveraging LPWAN for data transmission and blockchain for authentication and traceability. It enhances data availability and auditability but depends heavily on technology infrastructure for scalability. [18] Proposes a digitalization strategy for smart cities using blockchain to improve urban services and reduce resource consumption. It aims to optimize energy, water consumption, and waste management, although it requires significant technological infrastructure and faces implementation complexities. [19] Implements a smart city IoT system with IaaS cloud computing architecture and blockchain for enhanced security and scalability. It optimizes routing performance and reduces operational costs, but relies on virtual simulations for performance evaluations. [20] Develops a security architecture based on authentication and authorization using multi-chain blockchain and SDN for municipal smart cities. It enhances data reliability and security during collaborative tasks but requires managing heterogeneous network collaborations and controlling data flows effectively.

Reviewing the research studies [11]-[20] reveals that the integration of blockchain technology into smart city IoT systems effectively tackles key issues concerning security, transparency, efficiency, and scalability. However, it is crucial to systematically examine how these technologies interact and complement each other to create more robust and adaptable urban infrastructures. In this context, **security and privacy** emerge as critical areas where blockchain-based architectures, incorporating advanced consensus protocols and machine learning models, significantly enhance security and privacy [11], [14]. While utilizing Docker and PySpark can improve real-time data processing, addressing resource intensity and implementation complexity remains crucial [11], [14]. Moving to **transparency and efficiency**, integrating blockchain with decentralized storage systems such as IPFS, and employing smart contracts for automated governance brings substantial improvements in transparency and operational efficiency [12], [17]. Nonetheless, scalability challenges persist, necessitating solutions that effectively balance resource utilization and scalability [12], [17]. In terms of **scalability and performance**, decentralized networks using protocols like CoAP and blockchain, combined with IaaS cloud computing architectures, offer enhancements in scalability and performance [13], [19]. Addressing encryption complexities and optimizing virtual simulations is essential for achieving better scalability and performance [13], [19]. **Operational challenges** also play a significant role, particularly in developing secure digital governance platforms and enhancing data verifiability in edge–fog–cloud environments. Effective management of integration complexity and real-time verifiability is vital, and simplifying these processes, along with improving experimental evaluations, could help mitigate these challenges [15], [16]. Lastly, **implementation and infrastructure** considerations reveal that digitalization strategies and smart waste management systems using blockchain face significant implementation challenges and dependencies on technological infrastructure [18], [17]. Developing more flexible and cost-effective infrastructure solutions will be key to supporting broader adoption and enhancing operational efficiency [17], [18].

In conclusion, to advance smart city IoT systems, it is essential to leverage techniques that integrate security, transparency, efficiency, and scalability. Approaches that combine advanced blockchain protocols, decentralized storage, and cloud computing architectures show considerable promise [11], [12], [13], [19]. Addressing challenges related to scalability, resource use, and implementation complexity will be key to developing robust and adaptable smart city IoT systems [14], [15], [16], [17], [18], [20].

C. Blockchain for smart healthcare IoT systems

With the rapid advancement of IoT technologies in healthcare, blockchain has been increasingly recognized for its potential to enhance security, data integrity, and operational efficiency. Table VI summarizes the key aspects of previous research, including the descriptions of various approaches, the methodologies employed, the benefits realized, and the limitations encountered. This overview provides valuable insights into how blockchain technology is transforming healthcare IoT systems and the challenges that remain.

TABLE VI
STUDIES CARRIED OUT ON HEALTHCARE BASED ON BLOCKCHAIN TECHNOLOGY.

References	Objectives	Used Methods	Benefits	Limitations
[21]	To improve the efficiency and security of healthcare systems using IoT and blockchain technologies by addressing issues related to data management, patient engagement, fraud prevention, and cost accuracy in the healthcare sector.	-Implementing blockchain technology in healthcare to ensure data integrity and security. -Using Ethereum for faster transactions and database management in medical studies. -Developing a web-based healthcare system architecture with front-end and back-end components.	-Enhanced data security and privacy in healthcare systems. -Faster transaction processing using Ethereum in medical studies. -High success rate in detecting illegal IoT device behavior.	-Implementation and integration of blockchain technology can be complex and costly. -Potential scalability issues with blockchain systems in healthcare.

[23]	Develop a secure framework for IoT-enabled healthcare systems using blockchain technology, including user authentication and health status prediction. Address security concerns related to wearable healthcare devices and data access.	-Utilization of RP2-RSA algorithm for data security. -Feature selection using CF-SSOA algorithm. -Health status classification with ASR-ANN technique. -Implementation of blockchain for secure medical data storage.	-Enhanced security for medical data using blockchain. -User privacy protection. -High accuracy and security compared to baseline techniques.	-Data load and network failures.
[24]	Develop a blockchain-based trust management framework (BFT-IoMT) for detecting and isolating Sybil nodes in Internet of Medical Things (IoMT) networks to enhance security and reliability, particularly in healthcare applications.	-Blockchain technology for distributed trust management. -Fuzzy logic for trust calculation and Sybil node detection. -Trust calculation, topology lookup, clustering, and trust value propagation in the fog layer.	-Improved energy efficiency. -Enhanced Sybil attack detection. -High packet delivery ratio and throughput. -Scalability for diverse and expanding IoMT networks. -Secure storage.	-Network delay due to fog layer computations.
[25]	Develop a secure healthcare system integrating IoT, Blockchain, and IPFS technologies for remote patient monitoring, especially for chronic diseases.	-Blockchain network for data storage and access control, using smart contracts. -IPFS for off-chain encrypted health data storage. -Ethereum Blockchain-based proof of authority consensus algorithm (Clique PoA). -Proxy re-encryption for data encryption and secure sharing.	-Ensures data privacy and integrity through Blockchain, smart contracts, and proxy re-encryption. -Scalable data storage with IPFS. -Improved processing time with Clique PoA consensus. -Enhanced security compared to existing methods.	-Implementation complexity. -Dependency on the quality of data and rules for proxy re-encryption.
[26]	Develop an architecture for secure and authorized health data sharing, including patients' vital signs and medical reports, by leveraging Blockchain, Edge/Fog computing, and LoRaWAN technologies.	-Data communication from IoT devices to application and Blockchain platforms using a Fog-based LoRa gateway. -Utilized the Ethereum Blockchain network with smart contracts for secure data storage and transactions. -Integration of Edge and Fog layers for reliable performance.	-Improved data security and authorization for health data sharing. -Enhanced patient monitoring for health and medical safety. -Efficient storage using private-permissioned Blockchain and IPFS.	-High implementation costs. -Complexity in hardware and software implementation.
[27]	Propose an IoT-Blockchain integration architecture using Ethereum Blockchain for healthcare applications and address resource constraints and other challenges in IoT.	-Enhanced Rich-Thin-Client architecture (ERTCA) with rich and thin clients. -Ethereum private Blockchain network with PoW consensus. -Ethereum account system for client identification and privacy.	-Enhances connectivity between IoT and Blockchain. -Efficiency in healthcare management. -Provides privacy through Ethereum account system and decentralization.	-Limitations of Ethereum account mechanism. -Scalability issues.
[22]	Develop a group authentication framework for Internet of Medical Things (IoMT) systems in order to solve the security problems associated with the computing, storage and self-protection capabilities of IoMT devices.	- Use elliptic curve cryptography. -Shamir secret sharing algorithm and fog computing technologies based on the blockchain. - Simulation on the Ethereum platform and the Solidity language. - Performance evaluation using the Hyperledger Caliper tool. - Security analysis using the Automated Validation of Internet Security Protocols and Applications tool.	-Resistance to authentication attacks. - Lightweight, scalable group authentication. - High latency and throughput.	- A large number of devices reduces efficiency and security.
[28]	Develop a secure and lightweight access control system for fog-assisted IoT cloud-based electronic medical records sharing, addressing security and privacy concerns.	- Ciphertext-Policy Attribute-Based Encryption. - IoT data encryption and secure aggregation. - Use of fog computing and Outsourced encryption and decryption algorithms on fog nodes. - Lightweight policy update algorithm for IoT cloud environment. -Blockchain technology.	- High efficiency and scalability. - Decentralized authentication and auditing. - Reduction in communication and computation costs.	- Lack of full exploitation of fog computing capabilities.

[29]	Develop a novel framework (SecureMed) based on blockchain for privacy preservation in the Internet of Medical Things (IoMT) by implementing distributed authentication at edge cloudlets to enhance privacy protection.	- Authentication algorithm using public/private key matching to authenticate IoMT devices. - Interaction between IoMT devices and edge cloudlets using smart contracts. - Utilization of blockchain for privacy preservation and IoMT transaction management.	- Reduced cloud traffic by processing IoMT data locally at edge cloudlets. - Improved performance in terms of latency. - Privacy protection for IoMT devices.	-Costly implementation (implementation Requires cloudlet infrastructure).
[30]	Develop a secure and trusted architecture for the Internet of Medical Things (IoMT) using Blockchain technology.	-Integration of Blockchain with the Trusted Third Party to ensure data immutability and transparency. -Implementation of Proof-of-Work (PoW) consensus protocol for securing patient health records.	-Enhanced security and privacy (for sensitive medical data in IoMT). -Reduction of single-point failure risks (compared to centralized cloud-based systems). -Tamper-proof architecture (with open access to authorized nodes).	-Potential challenges in implementing the PoW mechanism.

After a careful analysis of the data presented in Table VI, we conclude that the studies [21]-[30] collectively address the integration of blockchain technology into IoT systems applied in healthcare. These studies employ diverse methodologies aimed at enhancing security, privacy, efficiency, and trust in healthcare environments. [21] Aims to improve the efficiency and security of healthcare systems using IoT and blockchain technologies. It focuses on issues such as data management, patient engagement, fraud prevention, and cost accuracy in the healthcare sector. By implementing blockchain for data integrity and security, using Ethereum for faster transactions, and developing a web-based healthcare system architecture, the study achieves enhanced data security and privacy. However, challenges include the complexity and potential scalability issues associated with blockchain systems in healthcare. [22] Introduces a group authentication framework for Internet of Medical Things (IoMT) systems. It addresses security issues related to the computing, storage, and self-protection capabilities of IoMT devices using elliptic curve cryptography and Shamir secret sharing algorithm on blockchain. The framework enhances security by resisting authentication attacks and achieving lightweight, scalable group authentication. However, the efficiency and security of the framework may be compromised by a large number of devices. [23] Develops a secure framework for IoT-enabled healthcare systems, focusing on user authentication and health status prediction. It utilizes the RP2-RSA algorithm for data security, CF-SSOA algorithm for feature selection, and ASR-ANN technique for health status classification. Blockchain technology is employed for secure medical data storage, ensuring enhanced security and privacy protection. Challenges include managing data loads and network failures during real-time operations. [24] Proposes a blockchain-based trust management framework (BFT-IoMT) for detecting and isolating Sybil nodes in IoMT networks. The framework employs blockchain for distributed trust management and fuzzy logic for trust calculation, and Sybil node detection. It enhances energy efficiency, Sybil attack detection, packet delivery ratio, and throughput in IoMT networks. However, network delay due to fog layer computations remains a limitation. [25] Introduces a secure healthcare system integrating IoT, blockchain and IPFS technologies for remote patient monitoring. The system uses blockchain for data storage and access control, employing smart contracts for automation and IPFS for off-chain encrypted health data storage. It adopts the Ethereum blockchain-based proof of authority consensus algorithm and proxy re-encryption for data encryption and secure sharing, ensuring data privacy and integrity. The approach improves security, scalability, and processing time compared to traditional methods but faces challenges in implementation complexity and dependency on data quality for proxy re-encryption. [26] Focuses on the authorized sharing of healthcare data in IoT applications. It explores blockchain's role in ensuring secure and authorized access to sensitive health data, enhancing data privacy and control. However, complexities in implementation and ensuring interoperability with existing healthcare systems are challenges. [27] Addresses privacy preservation in medical IoT applications. It proposes techniques to protect patient data privacy using blockchain, ensuring data integrity and confidentiality in medical IoT environments. Challenges include managing data access rights and ensuring compliance with healthcare regulations. [28] Develops a secure IoT-based framework for remote patient monitoring using blockchain technology. It enhances security by employing blockchain for secure data storage and access control, ensuring patient data privacy and integrity. The framework improves efficiency in healthcare delivery but faces challenges in scalability and real-time data processing. [29] Focuses on blockchain-based solutions for improving healthcare data management and interoperability. It proposes blockchain architectures to address data silos and enhance interoperability between healthcare systems, ensuring data security and efficiency. Challenges include the complexity of integrating blockchain with existing healthcare IT infrastructure and ensuring regulatory compliance. [30] Explores the application of blockchain in healthcare supply chain management. It addresses issues such as traceability, transparency, and efficiency in the healthcare supply chain by utilizing blockchain for secure and transparent data management. Challenges include scalability and ensuring the reliability of data across the supply chain network.

Analyzing the studies presented earlier [21]-[30] reveals that integrating blockchain technology into IoT systems within

healthcare addresses key challenges related to security, privacy, efficiency, and data management. However, it is crucial to systematically examine how these methodologies interact and complement each other to develop more robust, scalable, and adaptable healthcare IoT infrastructures. By focusing on the synergy between blockchain-based security enhancements, efficient data management frameworks, and scalable solutions, we can gain a deeper understanding of how to overcome the complexities and limitations associated with their implementation in healthcare environments. **Security and privacy** emerge as critical areas where implementing blockchain enhances data integrity, access control, and secure data storage, thereby improving security and privacy in healthcare systems [21], [23], [25]. However, challenges related to implementation complexity and scalability need to be addressed [21], [25]. When considering **efficiency and scalability**, blockchain-based frameworks such as BFT-IoMT for trust management and IoT-based frameworks for remote patient monitoring contribute to increased efficiency and scalability [24], [28]. Nevertheless, issues like network delays and real-time processing require effective solutions [24], [28]. In the domain of **data management and interoperability**, blockchain architectures that address data silos and improve interoperability between healthcare systems show promise for better data management [29]. Overcoming challenges related to integrating blockchain with existing IT infrastructure is essential for realizing these benefits [29]. **Implementation challenges** also play a significant role, as complexities in implementation and dependencies on technology quality are notable obstacles [25], [26]. Simplifying implementation processes and improving data quality management are crucial steps towards effective integration. Finally, **supply chain management** benefits from blockchain technology through enhanced traceability and transparency [30]. However, addressing scalability and ensuring data reliability across the supply chain are critical for successful implementation [30].

In conclusion, integrating blockchain technology into healthcare IoT systems provides significant improvements in security, privacy, and data management. Key benefits include enhanced data integrity and secure transaction processing through Ethereum [21], [23], and improved authentication and privacy using elliptic curve cryptography and IPFS [22], [25]. Additionally, innovations like fog computing and edge-based data sharing contribute to better patient monitoring [26], [28]. Nevertheless, challenges such as implementation complexity, scalability, and integration with existing systems remain. Addressing these issues is crucial for fully realizing blockchain's potential in healthcare IoT and developing more robust and adaptable systems [21], [26], [27].

D. Blockchain for Industrial IoT systems

In the quest to enhance the Industrial Internet of Things (IIoT), integrating blockchain technology has gained significant attention for its potential to address key challenges. Table VII encapsulates a comprehensive review of previous research efforts in this domain, detailing the various descriptions of blockchain applications, the methodologies employed, the advantages realized, and the limitations faced. This overview highlights the advancements achieved through blockchain integration and provides a basis for understanding the ongoing research landscape within IIoT.

TABLE VII
STUDIES CARRIED OUT ON INDUSTRIAL INTERNET OF THINGS BASED ON BLOCKCHAIN TECHNOLOGY.

References	Objectives	Used Methods	Benefits	Limitations
[31]	Address storage and scalability issues in Blockchain-IIoT integration by proposing a deep reinforcement learning (DRL) approach for block selection.	-Deep Reinforcement Learning (DRL) approach for block selection. -Conversion of multi-objective optimization into a Markov decision process (MDP). -Utilization of two DRL algorithms: Advantage Actor-Critic and Proximal Policy Optimization.	-Achieves substantial reduction in storage requirements for blockchain peers compared to full replication approach. -Faster runtime of DRL algorithms compared to benchmark evolutionary algorithms.	-Complexity in block selection decisions. -Need for evaluating cloud service costs.
[32]	Implement an Artificial Intelligence based Lightweight Blockchain Security Model (AILBSM) to enhance privacy and security of cloud-based Industrial Internet of Things (IIoT) systems.	-Combining lightweight blockchain and Convivial Optimized Sprinter Neural Network AI mechanisms for improved security operations. -Feature transformation using Authentic Intrinsic Analysis model to reduce the impact of attacks.	-Enhanced privacy and security for IIoT systems through the AILBSM framework. -Improved execution time, classification accuracy, and detection performance. -Enhanced anomaly detection performance compared to other techniques.	-Complexity in implementation and management.
[37]	Address security, resource utilization, latency, and reliability challenges in Industrial Internet of Things (IIoT) networks by proposing an energy-efficient blockchain-integrated Software-Defined Networking (SDN) architecture.	-Decentralized blockchain integration with SDN -A novel energy-aware cluster-head selection model.	-Better energy consumption -Homogeneous SDN controllers improve scalability, privacy	-High cost -Lack of an access control mechanism in the SDN.

[33]	Solve the challenges of sharing computing resources in fog networks, particularly in Industry 4.0, by proposing a new architecture called Blockchain-enabled Resource Sharing in Fog Networks .	-Partition a Fog system into Fog clusters. -Design Blockchain-enabled Resource Sharing inside Smart Machines in Fog networks.	-Secure and efficient computing resource sharing in fog networks. -Ensure consensus in an untrustworthy fog environment.	-Lacks consideration of computational overhead involved in dividing the fog network into clusters.
[34]	Propose an energy-efficient routing protocol for the Industrial Internet of Things (IIoT) with the integration of blockchain technology to enhance network performance and lifetime.	-Developed an Industrial IoT Fuzzy Logic Energy-Aware Routing Protocol. -Introduced a Multilayer Energy-Aware Routing Protocol cluster with three phases: network ring creation, intra-ring divisions, and inter-cluster routing. -Proposes Enhanced Mobility Support Routing Protocol using fuzzy logic for RSSI and PER metrics to handle mobility.	-Decreases network traffic and improves network lifetime. -Reduce identical data package transfers. -Reduce interruptions caused by mobility.	-The limited use of collector nodes could have negative implications.
[35]	Meet the challenges of low computing power in Industrial Internet of Things (IIoT) devices for federated learning by introducing edge computing, blockchain for data security and transfer learning to improve system performance.	-Comparative analysis of the proposed algorithm with CSE, GRAE, and FedAvg	-Feasibility of low computing power devices in IIoT participating in federated learning is verified. -Improved transfer learning accuracy in the proposed algorithm.	-Transfer learning accuracy is not high. -Data transmission encryption and decryption consume resources.
[36]	Designing a new IIoWT architecture for water management that guarantees the standardization, interoperability and security of data between the various institutions in the water sector.	- Digital twin-enabled cross-platform environment using MQTT protocol. - CNN Long Short-Term Memory and Blockchain Data Transactional scheme for processing valid data across different nodes in water management.	-Reduce data processing time. - Real-time monitoring. -Improve data integrity and accuracy.	- Scalability and power consumption issues.
[38]	Develop a trusted consortium blockchain framework to ensure big data integrity in IIoT environments.	-Trusted Consortium Blockchain framework. -Hyperledger Fabric Modular.	-Achieves strong data integrity. -High transaction throughput. -Low latency.	-Complexity of blockchain implementation and management.
[39]	Solve security and scalability issues related to permission operations in the Industrial Internet of Things (IIoT) by offering a decentralized access control management system based on smart contracts and privacy-preserving techniques.	-Utilize three smart contracts: Token Issue Contract, User Register Contract, and Manage Contract. -Post-quantum lightweight encryption algorithm for user privacy. -Encrypted Nth-degree Truncated Polynomial Ring Units .	-Enhances security and scalability -Preserves user privacy and control -Dynamic access control	-Implementation complexity -Monitor security (in real time)
[40]	Integrate BlockChain and Software Defined Networking (SDN) to Improve Cloud Security for Intelligent IIoT Applications	-Distributed Secure Blockchain Methodology, Cloud Computing Management, and Services for the smart IIoT applications. -Distributed blockchain method. - Software Defined Networking (SDN).	- Load balancing improvement. - Flexibility and scalability. - Enhanced security, secrecy, privacy and integrity.	- Complexity of integrating multiple technologies. - Overhead on network resources. -Performance overhead.

After a comprehensive analysis of the data presented in Table VII, the studies [31]-[40] collectively explore the integration of blockchain technology into the Industrial Internet of Things (IIoT), focusing on critical aspects such as storage efficiency, security enhancement, energy efficiency, resource sharing, routing protocols, federated learning, hardware security, big data integrity, access control, and cloud architecture. Each study employs unique methodologies tailored to address the specific challenges encountered in IIoT environments. [31] Proposes a deep reinforcement learning (DRL) approach for block selection in IIoT, aiming to reduce storage requirements significantly. The method converts multi-objective optimization into a Markov decision process (MDP) and utilizes DRL algorithms like Advantage Actor-Critic and Proximal Policy Optimization. Benefits include substantial reductions in storage requirements and faster runtime compared to traditional methods. However, it faces challenges such as complex block selection decisions and the need to evaluate cloud service costs. [32] Implements the Artificial Intelligence based Lightweight Blockchain Security Model (AILBSM) to enhance privacy and security in cloud-based IIoT systems. It combines lightweight blockchain and Convivial Optimized Sprinter Neural Network AI mechanisms, leveraging an Authentic Intrinsic Analysis model for attack mitigation. Benefits include enhanced execution time, classification accuracy, and anomaly detection performance. However, complexities in implementation and management are significant limitations. [33] Introduces blockchain-enabled resource sharing in fog networks to address resource sharing challenges in Industry 4.0. It partitions fog systems into clusters and implements blockchain-enabled resource sharing inside smart machines. While it ensures secure and efficient resource sharing, the study overlooks the computational overhead involved in

dividing the fog network into clusters. [34] Proposes an energy-efficient routing protocol for IIoT using fuzzy logic-based protocols. The protocol aims to enhance network performance and lifetime by reducing network traffic and interruptions caused by mobility. Benefits include improved network performance and lifetime, but limitations exist due to the limited use of collector nodes. [35] Tackles low computing power challenges in IIoT devices through federated learning and edge computing integration with blockchain. While verifying the feasibility of low computing power devices in federated learning, the study faces challenges in achieving high transfer learning accuracy and managing resource consumption during encryption and decryption. [36] Designs an IIoT architecture for water management, emphasizing data standardization, interoperability, and security across different nodes. It employs digital twin-enabled cross-platform environments and blockchain for data transactional integrity. Benefits include reduced data processing time and improved data integrity, yet scalability and power consumption remain significant issues. [37] Proposes an energy-efficient blockchain-integrated SDN architecture for IIoT networks to address security, latency, and reliability challenges. It introduces a decentralized blockchain integration with SDN and a novel energy-aware cluster-head selection model. While it improves energy consumption and scalability, limitations include high costs and the absence of an access control mechanism in SDN. [38] Develops a consortium blockchain framework to ensure big data integrity in IIoT environments. Utilizing Hyperledger Fabric Modular, the framework achieves strong data integrity, high transaction throughput, and low latency. Challenges include the complexity of blockchain implementation and management. [39] Addresses security and scalability in IIoT with a decentralized access control system based on smart contracts and privacy-preserving techniques. It introduces smart contracts for dynamic access control and a post-quantum lightweight encryption algorithm for user privacy. Benefits include enhanced security and scalability, but the study faces complexities in implementation and real-time security monitoring. [40] Integrates blockchain and SDN to enhance cloud security for IIoT applications, focusing on load balancing improvement, flexibility, scalability, and enhanced security, secrecy, and privacy. Challenges include the complexity of integrating multiple technologies and performance overhead on network resources.

Evaluating the studies reviewed [31]-[40], it is clear that the integration of blockchain technology into the Industrial Internet of Things (IIoT) leads to significant improvements in storage efficiency, security, resource management, and data integrity. However, a thorough examination of how these varied methodologies work together is essential for developing more robust and adaptable IIoT infrastructures. By exploring the synergy between storage optimization, security measures, resource management techniques, and emerging technologies such as federated learning and SDN, we can gain deeper insights into addressing the complexities and limitations associated with blockchain deployment in IIoT contexts. In terms of **storage and scalability**, techniques like DRL-based block selection [31] offer significant reductions in storage needs and improved runtime. However, addressing complexity and cost issues is necessary for optimizing these benefits [31]. For **privacy and security** enhancement, models such as AILBSM [32] and decentralized access control systems [39] provide substantial improvements. Nonetheless, overcoming challenges related to implementation complexity and real-time monitoring remains essential [32], [39]. When examining **resource management and efficiency**, blockchain-enabled resource sharing frameworks [33] and energy-efficient routing protocols [34] contribute to better resource management and network performance. Challenges such as computational overhead and limited node utilization need to be addressed to fully leverage these frameworks [33], [34]. In the realm of **federated learning and edge computing**, integrating blockchain with federated learning [35] shows promise for low-power devices. However, issues related to transfer learning accuracy and resource consumption must be resolved to enhance effectiveness [35]. Regarding **data management and integrity**, frameworks like trusted consortium blockchains [38] and digital twin-enabled architectures [36] significantly improve data management and integrity. Addressing scalability and management complexity will be crucial for optimizing these solutions [36], [38]. Finally, integration with cloud and SDN highlights that combining blockchain with SDN [40] enhances **security and scalability** but introduces complexity and performance overhead. Efficient integration strategies are needed to manage these aspects effectively [40].

In conclusion, the integration of blockchain technology into IIoT systems offers substantial advancements, particularly in storage efficiency, security enhancement, resource management, and data integrity, as highlighted in studies [31]-[40]. For instance, the application of deep reinforcement learning to optimize storage [31], the implementation of AI-based lightweight blockchain security models [32], and the development of energy-efficient routing protocols [34] demonstrate significant progress in enhancing IIoT infrastructures. However, the challenges of scalability, implementation complexity, and the integration of emerging technologies such as federated learning [35] and SDN [37], [40] must be carefully addressed. Additionally, issues related to computational overhead and power consumption [36], as well as the complexity of managing blockchain networks [38], underline the need for continued research. Overcoming these challenges will be crucial in fully realizing the potential of blockchain to advance Industrial IoT environments and create more robust, scalable, and adaptable infrastructures.

E. Blockchain for smart agriculture IoT systems

As smart agriculture continues to evolve, the integration of blockchain technology into IoT systems promises to revolutionize the field by enhancing various aspects of agricultural management. Table VIII provides a detailed overview of prior research efforts that investigate this integration. It outlines the descriptions of blockchain applications, the methods utilized in these studies, the benefits achieved, and the limitations encountered.

TABLE VIII
STUDIES CARRIED OUT ON INTELLIGENT AGRICULTURAL BASED ON BLOCKCHAIN TECHNOLOGY.

References	Objectives	Used Methods	Benefits	Limitations
[50]	Develop a concept for the application of integrated digital technologies to enhance future smart and sustainable agricultural systems.	-Application of edge computing involves placing of service provisioning, data, and intelligence closer. -AI application for data integration and analysis. -Blockchain technology and smart contract cloud. -Decision support system.	-Improved data collection, management, and sharing. -Increased productivity and monitoring capabilities. -Enhanced economic performance.	-Challenges in integrating various digital technologies. -Complexity in managing different data formats and sources.
[44]	Explore the application of Blockchain, smart contracts, and IoT in re-engineering agricultural food supply chain.	-Business Process Modeling (BPM) to analyze the activities of the agriculture supply chain. -Incorporation of blockchain and smart contract-based findings into Reference Architecture for Modeling Industry 4.0 (RAMI 4.0). -Development, deployment, and testing of smart contracts using Solidity. -Implementation of hybrid smart algorithms using Ganache and Truffle.	-Enhanced transparency and visibility in supply chains. -Improved information security. -Real-time monitoring of product health and environment. -Automation of business processes.	-Interoperability and privacy issues.
[45]	Propose a fast and reliable storage method for agricultural IoT data based on blockchain to address issues of low efficiency in data collection and data storage security.	-RC5 (Rivest Cipher 5) encryption for data in IoT sensor module. -Aggregation of data batches in the gateway into a transaction. -Reconstruction of Merkle ordered tree for data integrity verification.	-Offers confidentiality, integrity, availability, controllability, and non-repudiation for information security. -Efficient storage security and credit guarantee for IoT data.	-Requires additional hardware overhead for data security calculations. -No processing of abnormal data before uploading to the blockchain.
[41]	Propose a model that combines agricultural expert knowledge, value chain planning through blockchain, and IoT technology to provide secure traceability in the hemp industry.	-Integration of agricultural expert knowledge (user-centered design). -Use of IoT protocols for traceability services (MQTT, HTTP, LoRaWAN). -Development of chain-codes (smart contracts) for different aspects of traceability. -IoT monitoring and control using sensors and actuators. -Cloud platforms (UBIDOTS, AWS) for data processing. -Hyperledger framework for blockchain integration. -Node-red programming for web interfaces and IoT data processing.	-Provides tamper-proof, transparent, and secure traceability. -Offers reliable monitoring and control through IoT devices.	-Requires careful integration of diverse technologies. -Initial development and implementation costs.
[43]	Propose a new blockchain architecture to ensure the integrity of agricultural data, improve data quality, and provide secure storage for farmers.	-Designing a multi-layered architecture integrating IoT sensors and blockchain. -Implementing smart contracts to automate processes and ensure data integrity. -Using a proof of concept (PoC) to demonstrate the feasibility of the proposed architecture.	-Ensures data integrity and authenticity by utilizing blockchain technology. -Automates processes through smart contracts. -Enhances supply chain transparency. -Secure storage and access to agricultural data.	-Dependency on technology advancements and user adoption for successful implementation.
[47]	Address key issues in the agriculture sector, including transparency, timeliness, traceability, security, and immutability, using blockchain technology by connecting various stakeholders through the usage of IoT devices and smart contracts in Ethereum	-Use of public key cryptography (RSA) for transaction encryption and verification. -Utilization of smart contracts in Ethereum.	-Enhances transparency, traceability, and security in the agriculture sector. -Reduces financial loss.	-Implementation complexity. -Dependence on IoT devices and the Ethereum blockchain may introduce vulnerabilities.

[46]	Design a security framework for smart agriculture (Agriculture 4.0) by combining blockchain technology, fog computing, and software-defined networking (SDN).	-Integration of blockchain technology, fog computing, and software-defined networking. -Simulations involving DDoS attacks (using Mininet and an open-source IoT platform (ThingsBoard)).	-Enhanced security for IoT-based agricultural systems. -Integration of blockchain ensures data integrity and transparency. -Fog computing optimizes processing and reduces latency for critical tasks.	-Complexity in integrating multiple technologies (blockchain, fog computing, SDN).
[49]	Propose a blockchain-based IoT model to improve supply chain transparency, traceability, and quality in agriculture.	-Implement smart contracts for automating transactions and improving trust among stakeholders -Energy-efficient routing approach for IoT-based agriculture.	.-Enhanced transparency and traceability in the supply chain. -Improved security and privacy. - Energy savings through the proposed routing approach.	-Potential scalability issues. -Complexity of implementing blockchain technology and integrating it with existing systems.
[42]	Investigate the potential role of blockchain technology in promoting smart farming by enhancing farming efficiency, lowering environmental impact, and automating farmers' work.	-Utilization of IPFS for off-chain data storage. -Asymmetric key exchange using ECC authentication algorithm and SHA-256 hashing. -Implementation of a secure blockchain-based framework using Ethereum. -Performance evaluation using Hyperledger Caliper.	-Enhanced efficiency and scalability in smart farming operations. -Improved data integrity and availability. -Data privacy through off-chain IPFS storage.	-Ethereum blockchain limitations in terms of performance and scalability.
[48]	Develop a secure data sharing framework for IoT-enabled Intelligent Agriculture, Utilize deep learning (DL) and smart contracts (SC) to enhance security.	-Deep Learning: Combining Convolutional Sparse Autoencoder with Gated Recurrent Units, Multi-Layer Perceptrons , and softmax classifier for intrusion detection. -Smart Contracts : Authentication, key management, transaction validation, mining using Smart Contracts based PoA consensus technique.	-Enhanced security through deep learning-based intrusion detection and transaction validation using smart contracts. -Secure data sharing among IoT-enabled Intelligent Agriculture entities. -Improved decision-making through agricultural yield prediction and quality enhancement via data analysis.	- Significant initial costs. - Complex implementation.

Following an in-depth analysis of the data set provided in Table VIII, the studies [41]-[50] collectively explore the integration of blockchain technology into intelligent agricultural systems based on the Internet of Things (IoT). These studies aim to enhance agricultural processes through various methodologies and techniques. [41] Proposes a model combining agricultural expert knowledge, blockchain value chain planning, and IoT for secure traceability in the hemp industry, emphasizing tamper-proof transparency and reliable monitoring. [42] Investigates blockchain's role in promoting smart farming by enhancing efficiency and scalability, leveraging IPFS for data storage and Ethereum for secure frameworks despite scalability limitations. [43] Introduces a new blockchain architecture to ensure data integrity and authenticity in agriculture, utilizing multi-layered approaches and smart contracts to automate processes and enhance supply chain transparency. [44] Explores blockchain, smart contracts, and IoT in re-engineering agricultural food supply chains, enhancing transparency, real-time monitoring, and business process automation despite interoperability challenges. [45] Proposes efficient storage methods for agricultural IoT data using blockchain, ensuring security and data integrity while facing hardware overhead and limitations in abnormal data processing. [46] Designs a security framework for Agriculture 4.0, integrating blockchain, fog computing, and SDN to enhance security, data integrity, and network management, despite complexities in technology integration. [47] Addresses transparency and traceability in agriculture using blockchain and IoT, highlighting improvements in security and reducing financial risks, yet facing complexities in implementation and dependency on IoT devices. [48] Develops a secure data sharing framework for IoT-enabled agriculture, combining deep learning for intrusion detection and smart contracts for transaction validation, despite initial costs and complex implementation. [49] Proposes a blockchain-based IoT model to enhance supply chain transparency and quality in agriculture, focusing on smart contracts and energy-efficient routing while addressing scalability and integration challenges. [50] Outlines integrated digital technologies to enhance future sustainable agricultural systems, utilizing edge

computing, AI, blockchain, and smart contracts for improved data management and economic performance, despite challenges in technology integration and data management.

Examining the studies [41]-[50] in Table VIII, it becomes apparent that integrating blockchain technology into IoT-based smart agricultural systems offers significant opportunities to improve various agricultural processes. To fully leverage the benefits of blockchain in agriculture, it is essential to systematically analyze how different methodologies and techniques interact. By focusing on crucial aspects such as traceability, transparency, efficiency, scalability, data integrity, and security, while also addressing challenges related to integration, complexity, and cost, a more robust and flexible agricultural IoT infrastructure can be established. This comprehensive approach will be instrumental in overcoming limitations and fully unlocking the potential of blockchain technology to transform agricultural systems. In terms of **traceability and transparency**, models like [41] and frameworks combining blockchain with smart contracts [44] offer significant improvements in agricultural supply chains. However, addressing issues related to technology integration and interoperability is essential for maximizing these benefits [41], [44]. For **efficiency and scalability**, approaches utilizing IPFS for data storage [42] and energy-efficient routing [49] contribute to better performance. Despite these advancements, challenges concerning blockchain's overall performance and scalability persist and need to be addressed [42], [49]. Regarding **data integrity and security**, blockchain architectures and frameworks [43], [45] play a crucial role in ensuring data integrity and security. Yet, complexities in hardware requirements and limitations related to processing abnormal data present ongoing challenges [43], [45]. When examining **integration and complexity**, the integration of blockchain with fog computing and SDN [46], along with the use of AI and edge computing [50], shows potential for enhanced security and data management. Nevertheless, the complexity of integrating multiple technologies and managing diverse data formats poses significant hurdles that must be overcome [46], [50]. Finally, addressing **cost and implementation challenges** is critical, as highlighted by studies like [48]. These studies note the enhanced security provided by deep learning and smart contracts but also emphasize significant initial costs and implementation complexities. Finding solutions to these issues is crucial for practical deployment [48].

In conclusion, integrating blockchain technology into smart agricultural IoT systems presents substantial benefits, particularly in enhancing traceability, efficiency, and data integrity, as evidenced by studies [41]-[50]. For example, the combination of blockchain with IoT protocols for secure traceability in agriculture [41], the development of blockchain frameworks for improving farming efficiency and reducing environmental impact [42], and the advancement of secure data storage methods [45] illustrate the potential of blockchain to revolutionize agricultural practices. However, significant challenges such as the complexity of integrating multiple technologies [46], potential scalability issues [49], and high initial implementation costs [48], [50] must be carefully addressed. Overcoming these challenges is crucial to fully harnessing the potential of blockchain technology in creating more efficient, transparent, and resilient agricultural IoT systems.

F. Blockchain for smart energy IoT systems

In exploring the integration of blockchain technology within smart energy systems, Table IX presents a concise overview of previous research efforts. This table summarizes the methodologies employed, the benefits achieved, and the limitations identified in past studies. By providing a snapshot of how blockchain can impact smart energy solutions, Table IX offers insights into both the advancements made and the areas that require further investigation and improvement.

.

TABLE IX
STUDIES CARRIED OUT ON SMART ENERGY BASED ON BLOCKCHAIN TECHNOLOGY

References	Objectives	Used Methods	Benefits	Limitations
[51]	Develop a new IoT architecture model for smart energy networks using blockchain and software-defined network (SDN) technology to address bandwidth constraints and trust issues in centralized smart energy network architectures.	-Integration of blockchain and SDN technology. -Implementation of the MTP-Argon2 hash function algorithm in the Itsuku PoW technical solution. -Network control right separation technology.	-Network load robustness. -Improves energy efficiency. -Low latency. -Improves security stability.	-High consumption of computing resources. -Complexity of implementation.
[52]	Develop a vehicle-to-everything blockchain power trading and energy management platform for multi-level power transactions in electric vehicle charging stations.	-Combination of artificial intelligence, Internet of things (IoT), and blockchain technology. -Smart contracts and distributed ledgers for power transactions. -Integration of communication protocols through artificial intelligence of things. -Energy management system for optimal scheduling.	-Reduces chaining latency. -Ensures security and fairness of data. -Automatically balances supply and demand.	-Centralized data processing for certain functions. -Limited decentralization in the blockchain technology.

[53]	Investigate unified coding and identification of smart grid IoT devices using blockchain technology and 5G MEC "Mobile Edge Computing" for efficient management and control.	-Combining blockchain technology with 5G MEC for connecting power IoT devices. -Analyzing consensus algorithms (PoW, PoS, DPoS, and PDFT) for feasibility in the hybrid blockchain mechanism based on 5G MEC.	-Improved privacy and efficiency in 5G networks. -Automation of transaction processes. -Cost savings and reduced transaction time. -Reliable and accurate management.	-Complexity and compatibility issues in implementation.
[54]	Propose a framework for implementing a blockchain-based microgrid system to manage various aspects of a microgrid system, including peer-to-peer (P2P) energy trading, Renewable Energy Certificate (REC) tracking, and decentralized energy trading.	-A decentralized blockchain network for storing energy data. -Consensus mechanism for verifying the authenticity of energy data. -Smart contracts for facilitating energy transactions. -Digital tokens for executing transactions.	-Increased transparency, efficiency, and security in energy trading and management. -Enhanced cybersecurity. -Improved reliability in energy generation and distribution.	-Increased transparency, efficiency, and security in energy trading and management. -Enhanced cybersecurity. -Improved reliability in energy generation and distribution.
[55]	Develop a Secure energy policy and load sharing for renewable microgrids	-Decentralized multi-agent system (MAS) for control. -Blockchain technology for data security. -Master-slave architecture in IoT and and cloud computing.	-Safe, automated, transparent, and economic operations in power distribution systems. -Resistance against malicious cyber-attacks. -Increased security of data measured in sensors and transaction data between agents.	-Complexity of implementing M-S organization and MAS. -Scalability issues of Blockchain technology.
[58]	Tackling the challenges of managing, controlling and operating smart grids and exploring the potential of blockchain-based solutions.	- Integration of blockchain technology with smart grid components, including synchro-phasor networks, IoT-enabled sensors, and decentralized control architectures. - Use of smart contracts for decentralized energy management and operation.	- Improved data availability and reliability. - Improved security and confidentiality of exchanges. - Increased efficiency of renewable energy resources. - Real-time measurements.	- Challenges related to scalability.
[56]	Design, implement, and test a peer-to-peer energy trading platform that harnesses the benefits of blockchain and IoT to enable decentralized, real-time, secure, and transparent energy trading.	- Use of the Ethereum blockchain for recording transactions. - ESP32-S2 microcontrollers for data collection. - MQTT protocol for data transfer. -Integration of IoT devices for energy control.	- Facilitates peer-to-peer energy trading. - Real-time monitoring and control of self-generated energy. - Tamper-proof recording of trading activities on the blockchain.	- Dependency on internet connectivity for platform operation.
[57]	Efficient energy management in the smart grid using Software-Defined Networking (SDN) and Digital Twin (DT), addressing communication vulnerabilities through blockchain authentication and implementing a Deep Learning (DL) based intrusion detection system.	- Use the blockchain-based authentication system to secure communication channels. - Use the DL architecture for intrusion detection. - Integration of DT technology into the SDN control plane to store smart meter operating states and behavior models.	-Improved detection of attacks. -Real-time and low-latency services. -Improved data analysis capabilities.	-Difficulty in guaranteeing secure and effective access control. -Unsecured channels at lower levels.
[59]	Design a blockchain-based local energy market, employing various methods including of IoT technologies, blockchain technologies, and consensus protocols.	-Blockchain technology for peer-to-peer network. -Application of Consensus Protocols in distributed ledger technologies. -Examine types of distributed ledger technologies, such as Tangle, Hash-graph, Sidechain. -Energy trading platforms based on blockchain.	-Real-time transaction processing. -Scalability. -Secure transactions.	-Limited transaction throughput in certain blockchains. -High energy consumption for the PoW protocol.

[60]	Explore the application of blockchain technology in managing a decentralized energy network with integrated distributed renewable energy sources by efficient consensus mechanisms for peer-to-peer energy sharing, transmission, data storage, and smart contracts.	-Implementing a permissioned blockchain system. -Using decentralized cloud storage. -Developing smart contracts. -Employing system controller/regulator.	-Enhanced security. -Peer-to-peer energy sharing. -Improved consensus mechanism. -Enhanced visibility and transparency.	-Expensive and Limited data storage on blockchain. -Privacy issues.

After careful examination of the data presented in Table IX, the studies [51]-[60] collectively focus on recent studies exploring the integration of blockchain technology within smart energy systems based on the Internet of Things (IoT). These studies employ diverse methodologies aimed at enhancing the efficacy, security, and transparency of smart energy networks. [51] Introduces an IoT architecture model integrating blockchain and Software-Defined Networking (SDN) to address bandwidth constraints and trust issues, highlighting benefits such as network load robustness and improved energy efficiency, despite challenges like high computing resource consumption. [52] Develops a blockchain-powered platform for vehicle-to-everything power trading and energy management, leveraging smart contracts and distributed ledgers to reduce latency, ensure data security, and automatically balance supply and demand, while facing limitations in centralized data processing. [53] Investigates unified coding and identification of smart grid IoT devices using blockchain and 5G Mobile Edge Computing (MEC), emphasizing improved privacy, efficiency, and cost savings, despite complexities in implementation and compatibility. [54] Proposes a blockchain-based microgrid system for peer-to-peer energy trading and Renewable Energy Certificate (REC) tracking, enhancing transparency and security in energy management, though facing challenges in scalability and technology adoption. [55] Develops a secure energy policy using blockchain and multi-agent systems for renewable microgrids, ensuring automated and transparent operations, and resistance against cyber-attacks, but faces complexity and scalability issues. [56] Implements a peer-to-peer energy trading platform using Ethereum blockchain and IoT devices, enabling decentralized trading and tamper-proof transaction recording dependent on stable internet connectivity. [57] Addresses smart grid management using SDN and Digital Twin technologies with blockchain-based authentication and intrusion detection systems, improving attack detection and real-time data analysis capabilities despite access control challenges. [58] Explores blockchain's potential in smart grid management, integrating synchrophasor networks and IoT sensors for improved data reliability and security, highlighting challenges in scalability and decentralized energy management. [59] Designs a blockchain-based local energy market for real-time transactions and secure energy trading, utilizing consensus protocols for scalability and secure transactions, yet facing throughput limitations and high energy consumption. [60] Examines a decentralized energy network managed by blockchain, enhancing security and peer-to-peer energy sharing through efficient consensus mechanisms and smart contracts, while addressing concerns over data storage and privacy.

Following a thorough analysis of the studies [51]-[60], a variety of methodologies have been employed to enhance the efficacy, security, and transparency of smart energy networks. The primary areas of exploration include energy efficiency, data security, scalability, and real-time decentralized trading, all of which are crucial for optimizing the performance and reliability of these systems. However, the studies also highlight significant challenges, such as computing resource consumption, scalability issues, integration complexity, and data management concerns. Addressing these challenges is essential to fully harnessing the potential of blockchain technology in advancing smart energy networks. In terms of **energy efficiency and management**, approaches like [51] and [52] demonstrate significant improvements in network efficiency and energy management through blockchain and IoT. However, addressing challenges related to computing resource consumption and centralized data processing is essential to fully leveraging these improvements [51], [52]. For **data security and privacy**, studies such as [53] and [54] show advancements in data security and transparency using blockchain. These approaches enhance privacy and security but face challenges related to scalability and compatibility, which must be overcome to ensure robust protection and performance [53], [54]. Regarding **scalability and integration**, frameworks and platforms like [55] and [58] offer solutions for scalable and efficient energy management. Despite these advancements, issues related to technology integration and scalability remain. Therefore, exploring solutions for real-time and decentralized trading becomes necessary to address these ongoing challenges [55], [58]. When examining **real-time and decentralized trading**, research such as [56] and [59] emphasizes the benefits of decentralized trading and real-time transactions. Nonetheless, limitations in throughput and energy consumption need to be addressed to optimize these benefits and support efficient trading mechanisms [56], [59]. Finally, in terms of **security and peer-to-peer sharing**, studies like [57] and [60] highlight the potential of blockchain to enhance security and enable peer-to-peer energy sharing. Addressing challenges related to access control, data storage, and cost is crucial for maximizing the effectiveness of these solutions [57], [60].

In conclusion, leveraging blockchain technology in smart energy IoT systems offers significant benefits in terms of efficiency, security, and transparency, as demonstrated by studies [51]-[60]. For example, the integration of blockchain with SDN and IoT improves network robustness and energy management [51], [52], while blockchain-based platforms enable secure peer-to-peer energy trading and real-time monitoring [56], [59]. Moreover, combining blockchain with technologies like 5G MEC enhances data integrity and system automation [53]. However, challenges such as scalability, integration complexity, and high implementation costs remain

[51], [55], [60]. Addressing these challenges is essential to fully harness the potential of blockchain for advancing smart energy networks

G. Synthesis of findings

The synthesis of findings from Tables IV to IX underscores a significant effort to integrate blockchain technology into various IoT domains, each aiming to address fundamental challenges and capitalize on blockchain's transformative potential. This discussion delves into the key advancements and persistent issues across different IoT ecosystems, providing a nuanced perspective on the current state of blockchain integration.

In the realm of smart home IoT systems, blockchain technology has been employed to enhance security, detect malicious activities, and prevent intrusions. Various methodologies have been explored:

Blockchain-based secure communication: Techniques that use blockchain to secure communication channels have demonstrated notable improvements in data protection and system integrity. These approaches leverage the immutability and decentralization properties of blockchain to provide a robust defense against unauthorized access and tampering [1], [2].

Machine learning techniques: Integrating machine learning with blockchain has shown promise in predicting and detecting potential threats. Machine learning algorithms can analyze patterns and anomalies, enhancing the system's ability to preemptively address security concerns [2], [5].

Lightweight authentication mechanisms: The use of ethereum blockchain and smart contracts for lightweight authentication mechanisms has been particularly effective. These methods reduce the overhead associated with traditional authentication methods while maintaining high security standards [3], [4], [6].

Despite these advancements, scalability and computational overhead remain pressing concerns. The energy consumption required for blockchain operations and the need for reliable node performance highlight the necessity for innovative solutions. Addressing these issues through optimized algorithms and energy-efficient protocols is crucial for the practical deployment of blockchain in smart home IoT systems [1], [6], [8].

The integration of blockchain into smart city IoT systems reflects a concerted effort to tackle urban challenges related to security, transparency, and privacy. Key advancements include:

Blockchain-based architectures: These architectures facilitate efficient data processing and enhance overall system performance. They enable decentralized data management, which improves transparency and reduces the risk of data manipulation [11], [12], [13].

Smart contracts for automated governance: The use of smart contracts has streamlined governance processes, automating routine tasks and reducing administrative overhead. This automation contributes to more efficient and responsive urban management [12], [16].

Privacy-protected data processing: Innovations such as homomorphic encryption have been employed to ensure privacy while allowing data processing. This technique supports secure data analysis without exposing sensitive information [14], [15].

Nevertheless, scalability and infrastructure dependencies present ongoing challenges. Integrating blockchain with existing city infrastructure and managing resource-intensive operations require sophisticated solutions. Efforts to enhance scalability and optimize resource management will be critical for the successful implementation of blockchain in smart cities [11], [13], [17].

In the healthcare sector, blockchain integration aims to improve security, privacy, and efficiency in managing patient data. Prominent methodologies include:

Encryption techniques: Advanced encryption methods ensure the confidentiality and integrity of sensitive patient information. These techniques are essential for protecting data from unauthorized access and breaches [21], [23].

Consensus algorithms: Consensus algorithms play a crucial role in maintaining data consistency and trust within the healthcare system. They enable secure and reliable transactions, which are vital for patient data management [24], [25].

Secure frameworks for patient data management: Frameworks that combine blockchain with other security measures provide comprehensive protection for patient data. These frameworks support secure storage, access control, and auditability [22], [25], [27].

Despite these advancements, scalability and implementation complexity are significant challenges. Handling large volumes of data and ensuring real-time operations require further research and development. Addressing these challenges will be essential for realizing the full potential of blockchain in healthcare [21], [26], [28].

In the IIoT domain, blockchain technology addresses diverse aspects such as storage efficiency, security, and resource sharing:

Deep reinforcement learning for block selection: This technique optimizes the selection of blocks in the blockchain, enhancing efficiency and performance [31].

AI-based security models: AI-driven security models improve threat detection and response, providing robust protection against cyber-attacks [32], [33].

Blockchain-enabled resource sharing in fog networks: This innovation facilitates resource sharing and coordination among distributed fog nodes, enhancing overall system efficiency [33].

While these solutions offer substantial benefits, they also pose implementation and management challenges. Effective strategies for deployment, particularly in managing computational overhead and ensuring optimal resource utilization, are essential for successful blockchain integration in industrial settings [31], [32], [37].

The integration of blockchain into intelligent agricultural systems aims to enhance data management and transparency:

Blockchain value chain planning: This approach ensures secure traceability of agricultural products, improving supply chain transparency and accountability [41], [42].

Smart contracts for automating agricultural Processes: Smart contracts automate various agricultural processes, streamlining operations and reducing the potential for errors [43], [44].

Interoperability and data format complexities present challenges that require meticulous attention. Efforts to streamline integration and manage costs are crucial for maximizing the benefits of blockchain in agriculture [45], [46], [48].

In smart energy systems, blockchain technology is explored to improve efficacy and transparency:

Blockchain-powered platforms for energy management: These platforms enable efficient management of energy resources and transactions, enhancing overall system performance [51], [52].

Peer-to-Peer energy trading systems: Blockchain facilitates decentralized energy trading, allowing users to buy and sell energy directly, which improves market efficiency [54], [56].

Secure energy policies for renewable micro-grids: Blockchain supports secure and transparent policies for managing renewable energy resources, enhancing trust and reliability [55], [57].

Despite the promising benefits, challenges such as resource consumption and integration complexities remain. Addressing these technical obstacles is crucial for the widespread adoption of blockchain in energy systems [51], [53], [60].

In conclusion, the integration of blockchain technology across various IoT landscapes highlights its transformative potential in enhancing security, privacy, efficiency, and transparency. However, persistent challenges related to scalability, integration complexity, and data management must be addressed through strategic research and innovative solutions. Continued efforts in these areas will be essential for realizing the full benefits of blockchain technology across different IoT applications.

VI. Challenges and Future Research Directions

The integration of blockchain technology into the IoT offers several benefits, including enhanced security, traceability of agreements, privacy, and transparency. These advantages provide potential solutions to numerous challenges within the IoT context. However, the incorporation of blockchain into resource-constrained environments presents particular challenges, as highlighted below.

A. Scalability

One of the key challenges in integrating blockchain technology into the IoT is scalability. As the IoT network expands and the number of connected devices grows, the volume of transactions becomes substantial. However, blockchain struggles to scale efficiently with this growth, mainly due to its consensus protocols, which require the approval of all participants for each transaction. Existing consensus algorithms, such as PoW and PoS, mandate that all nodes confirm transactions, leading to slower validation processes as the size of the IoT network increases.

B. Storage capacity

Integrating blockchain into the IoT eliminates the need for a central server to manage transactions, but it introduces the challenge of storing the blockchain ledger on IoT nodes. The limited storage capacity, memory constraints, and network connectivity issues of IoT devices pose significant hurdles. Current blockchain implementations struggle with low transactions per second, and the vast amount of data generated by IoT sensors further complicates storage management. To mitigate these challenges, one potential solution is to utilize cloud resources to handle the growing data storage demands within the IoT and decentralized blockchain environment.

C. Energy Consumption

The integration of blockchain into an IoT network requires significant energy to provide its specialized services. In an IoT environment, sensors communicate with a central sink sensor to transmit data collected from various devices. IoT networks deployed in such environments face a range of challenges, including short-range communication, high signal attenuation, exposure to ultraviolet radiation, and the high cost of sensor deployment. Despite extensive research efforts aimed at addressing blockchain's energy consumption, this issue remains a persistent challenge. When blockchain services are integrated into an IoT network, each service requires a substantial amount of energy per transaction, which can result in delays in transaction confirmation. As a result, energy consumption in blockchain-based IoT systems is a complex research problem that requires focused attention.

D. Cost

Deploying communication actuators and sensors in the IoT environment presents a significant challenge. The processes involved in the installation, maintenance, and management of these devices are complex and intricate. Moreover, IoT sensors are susceptible to damage, loss, or malfunction in harsh environments. Therefore, it is crucial to install sensors efficiently to minimize the effort required for reinstallation and maintenance. The introduction of blockchain technology into an IoT system not only increases the overall setup cost but also makes the solution comparatively expensive.

E. Computing Power

The diverse IoT ecosystem consists of a wide array of devices with varying levels of computing power. The primary motivation for integrating blockchain into the IoT environment is its enhanced security features. The blockchain's consensus mechanism removes the need for third-party intervention, significantly improving security. However, implementing this consensus algorithm requires substantial computing resources. Consequently, miners must utilize powerful computing systems. Given that most IoT devices have limited computing capabilities, deploying certain consensus algorithms, such as PoW, can be challenging. One potential solution is to incorporate devices with higher computing capacities into the IoT ecosystem to mitigate this issue.

F. Security and data privacy

The integration of blockchain technology into IoT applications presents several security challenges. While blockchain is well-known for its resistance to tampering in decentralized networks, it is not without vulnerabilities. One major concern is the potential for attacks against the consensus protocol, which could allow malicious actors with substantial computing resources to compromise the security of consensus mechanisms. For instance, Proof of Work blockchains, like

Bitcoin, can be susceptible if attackers gain control of more than half of the hashing power. Additionally, smart contracts, which are permanent and irreversible, may introduce their own vulnerabilities. As privacy protection becomes increasingly critical, it is essential to combine blockchain verification mechanisms with confidentiality measures to effectively manage open data. Cryptocurrencies can enhance confidentiality, while encryption ensures secure data accessibility and supports the scalability of smart contracts. To maintain resilience against cyber-attacks, IoT applications require continuous updates to adapt to evolving threats

G. *Quality of service*

Integrating blockchain into the IoT poses significant challenges regarding quality of service. While blockchain offers advantages in security and traceability, it also imposes performance and latency constraints. In an IoT environment where billions of devices continuously generate data in real time, maintaining optimal quality of service is crucial. The decentralized nature of blockchain and its consensus mechanisms can introduce delays in transaction validation, necessitating the development of solutions to minimize these delays while ensuring data integrity. Additionally, managing transaction fees on the blockchain is vital for maintaining affordability, especially in IoT contexts where low-value transactions are prevalent. In brief, successfully integrating blockchain into the IoT ecosystem while preserving quality of service presents a major challenge.

H. *Latency and Data Transfer*

Latency and data transfer represent significant challenges in integrating blockchain into the Internet of Things (IoT) environment. This issue is particularly critical in IoT, where speed is essential due to the vast amounts of real-time data generated by sensors and connected devices. The decentralized nature of transaction validation on the blockchain, especially with mechanisms like proof of work, can result in delays in data recording. Researchers must develop solutions to minimize these delays while ensuring data security. In summary, effectively managing latency and data transfer remains a major obstacle to the successful integration of blockchain into the IoT.

I. *Automate processes and transactions*

The integration of smart contracts into IoT applications through blockchain technology introduces challenges, including code, methods, and data residing at specific addresses, potential accidental issues, and the need for network validation. Ensuring the efficient and secure processing of smart contracts is vital, as real-world data feeds can present validation risks. While cloud computing and big data capabilities can enhance computational capacity and facilitate deeper data analysis, it is essential to address these challenges for successful integration.

J. *Migration from Legacy Systems*

Migrating from legacy IoT systems presents a significant opportunity to enhance security against data tampering and theft through the adoption of blockchain technology. However, integrating IoT and blockchain projects can be challenging due to the specialized skills required. This process involves defining stakeholders, data ownership, entry and exit conditions, and mechanisms for information sharing. Additionally, the necessary tools to build a blockchain ecosystem are still under development, adding complexity to the transition. Moving away from older systems can be costly and often necessitates expert assistance to address initial deployment challenges.

K. *Legal and regulatory aspects*

In the realm of law and regulation, blockchain faces several legal challenges during its early stages, primarily due to a lack of regulation and limited familiarity with blockchain solutions. A comprehensive understanding of blockchain's mechanics is crucial for strengthening regulations related to transactions. In the context of local government and social governance, technology and legal considerations are often viewed as interchangeable. Applications based on blockchain, such as smart contracts and distributed verification systems, have the potential to transcend both legal and technical limitations, paving the way for innovative governance models. These solutions can enhance equity, fairness, productivity, and work quality. Ultimately, the success of blockchain hinges on its ability to shape processes while maintaining legal validity.

VII. CONCLUSION

Blockchain technology is poised to revolutionize the next generation of the IoT. This study provides an overview of the integration between blockchain technology and the IoT model across various environments, while also analyzing existing efforts in this domain. It thoroughly examines the complexities of both IoT and blockchain technology, encompassing aspects such as security features, privacy considerations, consensus algorithms, and their comparative analyses. Furthermore, the research focuses on the integration of blockchain into the IoT model, addressing the associated techniques, benefits, and limitations. The findings indicate that blockchain technology holds significant potential for enhancing the security and privacy of data within IoT systems, thereby fostering the growth of IoT applications. However, it is essential to acknowledge that the deployment and implementation of blockchain for IoT are still in their infancy, necessitating ongoing research to tackle the challenges and complexities inherent in this integration. In this context, the study identifies key unresolved questions and future research directions that could benefit researchers interested in the convergence of blockchain and IoT.

REFERENCES

[1] S. Menon *et al.*, "Blockchain and Machine Learning Inspired Secure Smart Home Communication Network", *Sensors*, vol. 23, nº 13, p. 6132, juill. 2023, doi: 10.3390/s23136132.

[2] L. Almuqren, K. Mahmood, S. S. Aljameel, A. S. Salama, G. P. Mohammed, et A. A. Alneil, "Blockchain-Assisted Secure Smart Home Network Using Gradient-Based Optimizer With Hybrid Deep Learning Model", *IEEE Access*, vol. 11, p. 86999-87008, 2023, doi: 10.1109/ACCESS.2023.3303087.

[3] B. M. Yakubu, M. I. Khan, A. Khan, F. Jabeen, et G. Jeon,"Blockchain-based DDoS attack mitigation protocol for device-to-device interaction in smart home", *Digital Communications and Networks*, vol. 9, nº 2, p. 383-392, avr. 2023, doi: 10.1016/j.dcan.2023.01.013.

[4] M. S. Farooq, S. Khan, A. Rehman, S. Abbas, M. A. Khan, et S. O. Hwang, "Blockchain-Based Smart Home Networks Security

Empowered with Fused Machine Learning", *Sensors*, vol. 22, nº 12, p. 4522, juin 2022, doi: 10.3390/s22124522.

[5] F. Iqbal *et al.*, "Blockchain-Modeled Edge-Computing-Based Smart Home Monitoring System with Energy Usage Prediction", *Sensors*, vol. 23, nº 11, p. 5263, juin 2023, doi: 10.3390/s23115263.

[6] B. Liu, X. Yao, K. Guo, et P. Zhu, "Consortium Blockchain Based Lightweight Message Authentication and Auditing in Smart Home", *IEEE Access*, vol. 11, p. 68473-68485, 2023, doi: 10.1109/ACCESS.2023.3293401.

[7] A. R. Kairaldeen, N. F. Abdullah, A. Abu-Samah, et R. Nordin, "Data Integrity Time Optimization of a Blockchain IoT Smart Home Network Using Different Consensus and Hash Algorithms", *Wireless Communications and Mobile Computing*, vol. 2021, p. 1-23, nov. 2021, doi: 10.1155/2021/4401809.

[8] K. Liao, "Design of the Secure Smart Home System Based on the Blockchain and Cloud Service", *Wireless Communications and Mobile Computing*, vol. 2022, p. 1-12, janv. 2022, doi: 10.1155/2022/4393314.

[9] M. J. Baucas, S. A. Gadsden, et P. Spachos, "IoT-Based Smart Home Device Monitor Using Private Blockchain Technology and Localization", *IEEE Netw. Lett.*, vol. 3, nº 2, p. 52-55, juin 2021, doi: 10.1109/LNET.2021.3070270.

[10] A. Qashlan, P. Nanda, X. He, et M. Mohanty, "Privacy-Preserving Mechanism in Smart Home Using Blockchain", *IEEE Access*, vol. 9, p. 103651-103669, 2021, doi: 10.1109/ACCESS.2021.3098795.

[11] A. E. Bekkali, M. Essaaidi, et M. Boulmalf, "A Blockchain-Based Architecture and Framework for Cybersecure Smart Cities", *IEEE Access*, vol. 11, p. 76359-76370, 2023, doi: 10.1109/ACCESS.2023.3296482.

[12] A. U. R. Khan et R. W. Ahmad, "A Blockchain-Based IoT-Enabled E-Waste Tracking and Tracing System for Smart Cities", *IEEE Access*, vol. 10, p. 86256-86269, 2022, doi: 10.1109/ACCESS.2022.3198973.

[13] A. Aldribi et A. Singh, "Blockchain Empowered Smart Home: A Scalable Architecture for Sustainable Smart Cities", *Mathematics*, vol. 10, nº 14, p. 2378, juill. 2022, doi: 10.3390/math10142378.

[14] Z. Xihua, S. B. Goyal, M. Tesfayohanis, et C. Verma, "Blockchain-Based Privacy-Preserving Approach Using SVML for Encrypted Smart City Data in the Era of IR 4.0", *Journal of Nanomaterials*, vol. 2022, p. 1-8, juill. 2022, doi: 10.1155/2022/7463513.

[15] V. Malik *et al.*, "Building a Secure Platform for Digital Governance Interoperability and Data Exchange Using Blockchain and Deep Learning-Based Frameworks", *IEEE Access*, vol. 11, p. 70110-70131, 2023, doi: 10.1109/ACCESS.2023.3293529.

[16] C. Martinez-Rendon, J. L. González-Compeán, D. D. Sánchez-Gallegos, et J. Carretero, "CD/CV: Blockchain-based schemes for continuous verifiability and traceability of IoT data for edge–fog–cloud", *Information Processing & Management*, vol. 60, nº 1, p. 103155, janv. 2023, doi: 10.1016/j.ipm.2022.103155.

[17] R. H. Filho, D. C. B. De Sousa, W. A. De Brito, J. L. M. D. S. Chaves, E. L. Sá, et V. P. D. A. Ribeiro, "Increasing Data Availability for Solid Waste Collection Using an IoT Platform based on LoRaWAN and Blockchain", *Procedia Computer Science*, vol. 220, p. 119-126, 2023, doi: 10.1016/j.procs.2023.03.018.

[18] I. Lukić, K. Miličević, M. Köhler, et D. Vinko, "Possible Blockchain Solutions According to a Smart City Digitalization Strategy", *Applied Sciences*, vol. 12, nº 11, p. 5552, mai 2022, doi: 10.3390/app12115552.

[19] S. Bommu *et al.*, "Smart City IoT System Network Level Routing Analysis and Blockchain Security Based Implementation", *J. Electr. Eng. Technol.*, vol. 18, nº 2, p. 1351-1368, mars 2023, doi: 10.1007/s42835-022-01239-4.

[20] S. Siddiqui, S. Hameed, S. A. Shah, A. K. Khan, et A. Aneiba, "Smart contract-based security architecture for collaborative services in municipal smart cities", *Journal of Systems Architecture*, vol. 135, p. 102802, févr. 2023, doi: 10.1016/j.sysarc.2022.102802.

[21] A. I. Taloba *et al.*, "A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare", *Alexandria Engineering Journal*, vol. 65, p. 263-274, févr. 2023, doi: 10.1016/j.aej.2022.09.031.

[22] N. Alsaeed, F. Nadeem, et F. Albalwy, "A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing", *Future Generation Computer Systems*, vol. 151, p. 162-181, févr. 2024, doi: 10.1016/j.future.2023.09.032.

[23] M. Kumar *et al.*, "BBNSF: Blockchain-Based Novel Secure Framework Using RP2-RSA and ASR-ANN Technique for IoT Enabled Healthcare Systems", *Sensors*, vol. 22, nº 23, p. 9448, déc. 2022, doi: 10.3390/s22239448.

[24] S. E. Ali, N. Tariq, F. A. Khan, M. Ashraf, W. Abdul, et K. Saleem, "BFT-IoMT: A Blockchain-Based Trust Mechanism to Mitigate Sybil Attack Using Fuzzy Logic in the Internet of Medical Things", *Sensors*, vol. 23, nº 9, p. 4265, avr. 2023, doi: 10.3390/s23094265.

[25] K. Azbeg, O. Ouchetto, et S. Jai Andaloussi, "BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security", *Egyptian Informatics Journal*, vol. 23, nº 2, p. 329-343, juill. 2022, doi: 10.1016/j.eij.2022.02.004.

[26] B. Dammak, M. Turki, S. Cheikhrouhou, M. Baklouti, R. Mars, et A. Dhahbi, "LoRaChainCare: An IoT Architecture Integrating Blockchain and LoRa Network for Personal Health Care Data Monitoring", *Sensors*, vol. 22, nº 4, p. 1497, févr. 2022, doi: 10.3390/s22041497.

[27] M. R. Bataineh, W. Mardini, Y. M. Khamayseh, et M. M. B. Yassein, "Novel and Secure Blockchain Framework for Health Applications in IoT", *IEEE Access*, vol. 10, p. 14914-14926, 2022, doi: 10.1109/ACCESS.2022.3147795.

[28] S. Fugkeaw, L. Wirz, et L. Hak, "Secure and Lightweight Blockchain-Enabled Access Control for Fog-Assisted IoT Cloud Based Electronic Medical Records Sharing", *IEEE Access*, vol. 11, p. 62998-63012, 2023, doi: 10.1109/ACCESS.2023.3288332.

[29] W. Rafique, M. Khan, S. Khan, et J. S. Ally, "SecureMed: A Blockchain-Based Privacy-Preserving Framework for Internet of Medical Things", *Wireless Communications and Mobile Computing*, vol. 2023, p. 1-14, avr. 2023, doi: 10.1155/2023/2558469.

[30] A. Bhattacharjya, K. Kozdrój, G. Bazydło, et R. Wisniewski, "Trusted and Secure Blockchain-Based Architecture for Internet-of-Medical-Things", *Electronics*, vol. 11, nº 16, p. 2560, août 2022, doi: 10.3390/electronics11162560.

[31] N. K. Akrasi-Mensah *et al.*, "Adaptive Storage Optimization Scheme for Blockchain-IIoT Applications Using Deep Reinforcement Learning", *IEEE Access*, vol. 11, p. 1372-1385, 2023, doi: 10.1109/ACCESS.2022.3233474.

[32] S. Selvarajan *et al.*, "An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems", *J Cloud Comp*, vol. 12, nº 1, p. 38, mars 2023, doi: 10.1186/s13677-023-00412-y.

[33] S. Rani, D. Gupta, N. Herencsar, et G. Srivastava, "Blockchain-enabled cooperative computing strategy for resource sharing in fog networks", *Internet of Things*, vol. 21, p. 100672, avr. 2023, doi: 10.1016/j.iot.2022.100672.

[34] A. Mehbodniya *et al.*, "Energy-Aware Routing Protocol with Fuzzy Logic in Industrial Internet of Things with Blockchain Technology", *Wireless Communications and Mobile Computing*, vol. 2022, p. 1-15, janv. 2022, doi: 10.1155/2022/7665931.

[35] P. Zhang, H. Sun, J. Situ, C. Jiang, et D. Xie, "Federated Transfer Learning for IIoT Devices With Low Computing Power Based on Blockchain and Edge Computing", *IEEE Access*, vol. 9, p. 98630-98638, 2021, doi: 10.1109/ACCESS.2021.3095078.

[36] M.A. Mohammed, A. Lakhan, K.H. Abdulkareem et al "Industrial Internet of Water Things architecture for data standarization based on blockchain and digital twin technology" , Journal of Advanced Research, 2023, doi:10.1016/j.jare.2023.10.005.

[37] S. Asaithambi *et al.*, "An Energy-Efficient and Blockchain-Integrated Software Defined Network for the Industrial Internet of Things", *Sensors*, vol. 22, nº 20, p. 7917, oct. 2022, doi: 10.3390/s22207917.

[38] M. Juma, F. Alattar, et B. Touqan, "Securing Big Data Integrity for Industrial IoT in Smart Manufacturing Based on the Trusted Consortium Blockchain (TCB)", *IoT*, vol. 4, nº 1, p. 27-55, févr. 2023, doi: 10.3390/iot4010002.

[39] W. Wang, H. Huang, Z. Yin, T. R. Gadekallu, M. Alazab, et C. Su, "Smart contract token-based privacy-preserving access control system for industrial Internet of Things", *Digital Communications and Networks*, vol. 9, nº 2, p. 337-346, avr. 2023, doi: 10.1016/j.dcan.2022.10.005.

[40] A. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, et P. Tiwari, "Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT", *Digital Communications and Networks*, vol. 9, nº 2, p. 411-421, avr. 2023, doi: 10.1016/j.dcan.2022.11.003.

[41] F.-J. Ferrández-Pastor, J. Mora-Pascual, et D. Díaz-Lajara, "Agricultural traceability model based on IoT and Blockchain: Application in industrial hemp production", *Journal of Industrial*

Information Integration, vol. 29, p. 100381, sept. 2022, doi: 10.1016/j.jii.2022.100381.

[42] K. S. Alqarni, F. A. Almalki, B. O. Soufiene, O. Ali, et F. Albalwy, "Authenticated Wireless Links between a Drone and Sensors Using a Blockchain: Case of Smart Farming", *Wireless Communications and Mobile Computing*, vol. 2022, p. 1-13, sept. 2022, doi: 10.1155/2022/4389729.

[43] A. El Mane, Y. Chihab, K. Tatane, et R. Korchiyne, "Agriculture Supply Chain Management Based on Blockchain Architecture and Smart Contracts", *Applied Computational Intelligence and Soft Computing*, vol. 2022, p. 1-23, oct. 2022, doi: 10.1155/2022/8011525.

[44] Z. Raza, I. U. Haq, et M. Muneeb, "Agri-4-All: A Framework for Blockchain Based Agricultural Food Supply Chains in the Era of Fourth Industrial Revolution", *IEEE Access*, vol. 11, p. 29851-29867, 2023, doi: 10.1109/ACCESS.2023.3259962.

[45] Y. Zhao, Q. Li, W. Yi, et H. Xiong, "Agricultural IoT Data Storage Optimization and Information Security Method Based on Blockchain", *Agriculture*, vol. 13, nº 2, p. 274, janv. 2023, doi: 10.3390/agriculture13020274.

[46] S. Padhy *et al.*, "AgriSecure: A Fog Computing-Based Security Framework for Agriculture 4.0 via Blockchain", *Processes*, vol. 11, nº 3, p. 757, mars 2023, doi: 10.3390/pr11030757.

[47] H. Patel et B. Shrimali, "AgriOnBlock: Secured data harvesting for agriculture sector using blockchain technology", *ICT Express*, vol. 9, nº 2, p. 150-159, avr. 2023, doi: 10.1016/j.icte.2021.07.003.

[48] R. Kumar, P. Kumar, A. Aljuhani, A. K. M. N. Islam, A. Jolfaei, et S. Garg, "Deep Learning and Smart Contract-Assisted Secure Data Sharing for IoT-Based Intelligent Agriculture", *IEEE Intell. Syst.*, vol. 38, nº 4, p. 42-51, juill. 2023, doi: 10.1109/MIS.2022.3201553.

[49] C. Intelligence And Neuroscience, "Retracted: Analysis of Agriculture and Food Supply Chain through Blockchain and IoT with Light Weight Cluster Head", *Computational Intelligence and Neuroscience*, vol. 2023, p. 1-1, juill. 2023, doi: 10.1155/2023/9834646.

[50] G. Gebresenbet *et al.*, "A concept for application of integrated digital technologies to enhance future smart agricultural systems", *Smart Agricultural Technology*, vol. 5, p. 100255, oct. 2023, doi: 10.1016/j.atech.2023.100255.

[51] J. Li, Y. Chen, Y. Chen, W. Zhang, et Z. Liu, "A smart energy IoT model based on the Itsuku PoW technology", *Results in Engineering*, vol. 18, p. 101147, juin 2023, doi: 10.1016/j.rineng.2023.101147.

[52] Y.-J. Lin, Y.-C. Chen, J.-Y. Zheng, D. Chu, D.-W. Shao, et H.-T. Yang, "Blockchain Power Trading and Energy Management Platform", *IEEE Access*, vol. 10, p. 75932-75948, 2022, doi: 10.1109/ACCESS.2022.3189472.

[53] D. Wang, H. Wang, et Y. Fu, "Blockchain-based IoT device identification and management in 5G smart grid", *J Wireless Com Network*, vol. 2021, nº 1, p. 125, déc. 2021, doi: 10.1186/s13638-021-01966-8.

[54] M. M. Khubrani et S. Alam, "Blockchain-Based Microgrid for Safe and Reliable Power Generation and Distribution: A Case Study of Saudi Arabia", *Energies*, vol. 16, nº 16, p. 5963, août 2023, doi: 10.3390/en16165963.

[55] W. Xu, J. Li, M. Dehghani, et M. GhasemiGarpachi, "Blockchain-based secure energy policy and management of renewable-based smart microgrids", *Sustainable Cities and Society*, vol. 72, p. 103010, sept. 2021, doi: 10.1016/j.scs.2021.103010.

[56] M. J. A. Baig, M. T. Iqbal, M. Jamil, et J. Khan, "Design and implementation of an open-Source IoT and blockchain-based peer-to-peer energy trading platform using ESP32-S2, Node-Red and, MQTT protocol", *Energy Reports*, vol. 7, p. 5733-5746, nov. 2021, doi: 10.1016/j.egyr.2021.08.190.

[57] K. Prabhat, K. Randhir, A. Ahamed, et al. "Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity", Solar Energy, vol. 263, p. 111921, 2023, doi: 10.1016/j.solener.2023.111921.

[58] L. Douiri, O. Samir, K. Sana, et al. "Energy Management Control and Operations in Smart Grids: Leveraging Blockchain Technology for Enhanced Solutions", Procedia Computer Science, vol. 224, p. 306-313 , 2023, doi: 10.1016/j.procs.2023.09.041

[59] H. Vahid, H. Barry, O. Brian, et al. "Practical Insights to Design a Blockchain-Based Energy Trading Platform", IEEE Access, vol. 9, p. 154827-154844, 2021. doi: 10.1109/ACCESS.2021.3127890.

[60] D. Oliver, M. Bessie, et S. Lindokhuhle. "Proposed framework for blockchain technology in a decentralised energy network", Protection and Control of Modern Power Systems, vol. 6, no 3, p. 1-11, 2021, doi: 10.1186/s41601-021-00209-8.

[61] M. A. Uddin, A. Stranieri, I. Gondal, et V. Balasubramanian, "A survey on the adoption of blockchain in IoT: challenges and solutions", Blockchain: Research and Applications, vol. 2, no 2, p. 100006, juin 2021, doi: 10.1016/j.bcra.2021.100006.

[62] E. A. Shammar, A. T. Zahary, et A. A. Al-Shargabi, "A Survey of IoT and Blockchain Integration: Security Perspective", IEEE Access, vol. 9, p. 156114-156150, 2021, doi: 10.1109/ACCESS.2021.3129697.

[63] A. A. Sadawi, M. S. Hassan, et M. Ndiaye, "A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges", IEEE Access, vol. 9, p. 54478-54497, 2021, doi: 10.1109/ACCESS.2021.3070555.

[64] A. Abdelmaboud et al., "Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions", Electronics, vol. 11, no 4, p. 630, févr. 2022, doi: 10.3390/electronics11040630.

[65] A. Alkhateeb, C. Catal, G. Kar, et A. Mishra, "Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review", Sensors, vol. 22, no 4, p. 1304, févr. 2022, doi: 10.3390/s22041304.

[66] R. Kumar et R. Sharma, "Leveraging blockchain for ensuring trust in IoT: A survey", Journal of King Saud University - Computer and Information Sciences, vol. 34, no 10, p. 8599-8622, nov. 2022, doi: 10.1016/j.jksuci.2021.09.004.

[67] H. D. Zubaydi, P. Varga, et S. Molnár, "Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review", Sensors, vol. 23, no 2, p. 788, janv. 2023, doi: 10.3390/s23020788.

[68] S. Tanwar, N. Gupta, C. Iwendi, K. Kumar, et M. Alenezi, "Next Generation IoT and Blockchain Integration", Journal of Sensors, vol. 2022, p. 1-14, août 2022, doi: 10.1155/2022/9077348.

[69] V. Gugueoth, S. Safavat, S. Shetty, et D. Rawat, "A review of IoT security and privacy using decentralized blockchain techniques", Computer Science Review, vol. 50, p. 100585, nov. 2023, doi: 10.1016/j.cosrev.2023.100585.

[70] Z. Hussein, M. A. Salama, et S. A. El-Rahman, "Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms", Cybersecurity, vol. 6, no 1, p. 30, nov. 2023, doi: 10.1186/s42400-023-00163-y.

[71] L. Javed, B. M. Yakubu, M. Waleed, Z. Khaliq, A. B. Suleiman, et N. G. Mato, "BHC-IoT: A Survey on Healthcare IoT Security Issues and Blockchain-Based Solution", IJECER, vol. 2, no 4, p. 1-9, déc. 2022, doi: 10.53375/ijecer.2022.302.

[72] C. Pujari, "A Novel Method of Secure Child Adoption Using Blockchain Technology", IAENG International Journal of Applied Mathematics, vol. 53, no 4, pp 1531-1539, 2023.

[73] A. Rghioui, S. Bouchkaren, et A. Khannous, "Blockchain-based Electronic Healthcare Information System Optimized for Developing Countries", IAENG International Journal of Computer Science, vol. 49, no 3, pp 833-847, 2022.

[74] A. A. Yaseen, K. Patel, A. A. Yassin, A. J. Aldarwish, et H. A. Hussein, "Secure Electronic Healthcare Record Using Robust Authentication Scheme", IAENG International Journal of Computer Science, vol. 50, no 2, pp 468-476, 2023.

[75] S. K. Dwivedi, P. Roy, C. Karda, S. Agrawal, et R. Amin, "Blockchain-Based Internet of Things and Industrial IoT: A Comprehensive Survey", Security and Communication Networks, vol. 2021, p. 1-21, août 2021, doi: 10.1155/2021/7142048.

[76] A. Ayub Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, et S. Kot, "Internet of Things (IoT) Security With Blockchain Technology: A State-of-the-Art Review", IEEE Access, vol. 10, p. 122679-122695, 2022, doi: 10.1109/ACCESS.2022.3223370.

[77] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, et I. Kantzavelou, "IoT: Communication protocols and security threats", Internet of Things and Cyber-Physical Systems, vol. 3, p. 1-13, 2023, doi: 10.1016/j.iotcps.2022.12.003.

[78] N. Alsaeed, F. Nadeem, et F. Albalwy, "A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing", Future Generation Computer Systems, vol. 151, p. 162-181, févr. 2024, doi: 10.1016/j.future.2023.09.032.