big data and cognitive computing

Review

Exploring IoT and Blockchain: A Comprehensive Survey on Security, Integration Strategies, Applications and Future Research Directions

Muath A. Obaidat [1,*], Majdi Rawashdeh [2,3], Mohammad Alja'afreh [4], Meryem Abouali [5], Kutub Thakur [6] and Ali Karime [7]

[1] Department of Computer Science, John Jay College and the Graduate School and University Center, City University of New York, New York, NY 10016, USA
[2] Department of Business Information Technology, Princess Sumaya University for Technology, Amman P.O. Box 1438, Jordan; m.rawashdeh@psut.edu.jo
[3] Department of Software Engineering, College of Engineering and Architecture, Al Yamamah University, Riyadh P.O. Box 45180, Saudi Arabia
[4] IoT Program, Department Communication Engineering, Princess Sumaya University for Technology, Amman P.O. Box 1438, Jordan; m.aljaafreh@psut.edu.jo
[5] Department of Computer Science, John Jay College, New York, NY 10019, USA; mabouali@jjay.cuny.edu
[6] Department of Professional Security Studies, New Jersey City University, Jersey City, NJ 07305, USA; kthakur@njcu.edu
[7] Electrical and Computer Engineering, Royal Military College of Canada, Station Forces, P.O. Box 17000, Kingston, ON K7K 7B4, Canada; ali.karime@rmc-cmr.ca
* Correspondence: muobaidat@ccny.cuny.edu or mobaidat@jjay.cuny.edu

Abstract: The rise of the Internet of Things (IoT) has driven significant advancements across sectors such as urbanization, manufacturing, and healthcare, all of which are focused on enhancing quality of life and stimulating the global economy. This survey offers an in-depth analysis of the integration of blockchain technology with IoT, addressing aspects such as architectural alignment, applications, security, limitations, scalability, and latency. Moreover, this survey focuses on security, integration techniques, and future research directions. The primary contributions of this review include a taxonomy of security concerns specific to IoT, an analysis of integration methods, and insights into consensus mechanisms suitable for resource-constrained environments. These findings highlight the unique challenges and opportunities in IoT–blockchain integration, providing a foundation for advancing secure and scalable IoT applications. By exploring consensus mechanisms and resource-constrained deployments, this paper provides a framework for developing secure and efficient IoT applications utilizing blockchain technology and providing a basis for future research and practical applications. In addition, this survey investigates innovative trends, including AI-driven blockchain for IoT.

Keywords: blockchain integration; IoT security; security; privacy; cyberattacks; smart devices; distributed ledger technology

Citation: Obaidat, M.A.; Rawashdeh, M.; Alja'afreh, M.; Abouali, M.; Thakur, K.; Karime, A. Exploring IoT and Blockchain: A Comprehensive Survey on Security, Integration Strategies, Applications and Future Research Directions. *Big Data Cogn. Comput.* **2024**, *8*, 174. https://doi.org/10.3390/bdcc8120174

Academic Editor: Omar Darwish and Yahya Tashtoush

Received: 11 September 2024
Revised: 17 November 2024
Accepted: 20 November 2024
Published: 28 November 2024

1. Introduction

The explosive growth in IoT deployments has brought about significant security and privacy challenges due to its reliance on centralized data storage, which is vulnerable to data breaches. The decentralized and tamper-resistant properties of blockchains present a potential solution to these challenges, offering a secure framework for data handling in the IoT. This study aims to provide a comprehensive survey of IoT–blockchain integration and to analyze the unique requirements, challenges, and solutions that arise when these two technologies intersect [1,2]

The purpose of IoT technology goes beyond improving people's day-to-day experiences; it also aims to strengthen the global economy by advancing multiple sectors [3–5].

However, the growing number of IoT devices has led to notable challenges in ensuring privacy and security [6–9]. According to several sources, including Forbes, ITSG Global, and LinkedIn, the total number of IoT devices is projected to exceed 207 billion by the end of 2024 [9,10]. These devices gather a wide array of data, typically stored on centralized servers, which raises issues about data security and trustworthiness [11–15].

IoT devices face several challenges, including the need for management by multiple administrators and the risk of unencrypted serves, which can lead to data breaches [16–18]. Blockchain technology offers a new way to serve decentralized storage and manage data. It uses a shared, secured, and distributed ledger to store and protect data without a centralized system, eliminating the need for third-party collectors [9–20]. Furthermore, blockchain allows devices to communicate and exchange based on the technology's decentralized, immutable, and shared nature along with its use of encrypted databases, which helps to provide security against various attacks [20–25]. One of the classic ways of collecting data from IoT devices is storage in centralized locations such as cloud servers [1,2,4,12]. Data storage in the cloud has led to a lack of trust in IoT devices, resulting in a push for the development of trusted decentralized servers where sensitive and private data can be safely stored [13–15]. IoT devices can face various challenges; some need to be managed by more than one manager simultaneously, while others may utilize an unencrypted server [16], which can lead to data being hacked and sensitive personal information being published [7,18].

When it comes to protection, blockchain technology is a new way to secure decentralized storage and data management. The concept on which it works is that of a shared, secure, and distributed ledger that stores and keeps safe all records and data without the need for a centralized system or third-party collector [19,20]. Blockchain allows two or more devices to communicate and exchange information, resources, and all sorts of data in a decentralized network, known as a peer-to-peer network [21–23]. Blockchain technology is decentralized, immutable, and shared; it uses a database ledger that stores and registers the data and transactions in the network [20,24].

Blockchain also helps to protect against various attacks, as the goal is to control a centralized system and gain control over personal information and other valuable data [20,25]. Another advantage of using Blockchain in IoT devices is that blockchain networks are encrypted, which in a P2P network means that every node is equipped with two different keys: a public key used by other nodes to encrypt messages [2,12], and a private key used to decrypt received message [2,12,20,26]. Despite its origins in cryptocurrency, blockchain technology is increasingly being used in IoT applications due to its security features [27,28].

The rapid expansion of the IoT has introduced complex security and privacy challenges due to reliance on centralized data management. Blockchain technology, with its decentralized structure and secure data handling, offers a promising solution to these challenges. This paper seeks to address these gaps by reviewing the integration methods, security implications, and performance constraints of IoT–blockchain systems, providing a comprehensive perspective on secure IoT applications.

1.1. Contributions

While past studies on blockchain and IoT have highlighted general applications, this survey specifically addresses integration methods and security concerns unique to IoT. Notably, earlier studies lack a thorough examination of consensus mechanisms suited to the resource limitations of IoT, and many do not analyze specific challenges associated with IoT–blockchain interaction. This paper fills these gaps by providing a comprehensive taxonomy of integration strategies, a comparison of consensus mechanisms, an analysis of practical constraints, and a foundation for advancing secure IoT–blockchain integration. Our findings contribute a valuable perspective on how these technologies can be effectively combined to address emerging security needs in IoT applications. The main contributions of this paper are as follows.

- An overview of blockchain technologies, including components, features, and characteristics of blockchain and secure application methods.
- A focus on how blockchain can be integrated into the Internet of Things (IoT) infrastructure, including a discussion of recent methods and examples.
- A summary of blockchain applications in IoT along with implementation methods and requirements for integration.
- A discussion of blockchain security and how it can protect IoT from cyberattacks, with suggestions and protective measures.
- An exploration of the most suitable methods for IoT-blockchain integration, architectural challenges, and issues, along with an overview of consensus protocols and algorithms.
- A taxonomy detailing the security considerations and constraints involved in the IoT–blockchain integration process, aiming towards the establishment of a secure authentication framework.

1.2. Organization of the Paper

The rest of this paper follows a structured organization, beginning with an in-depth introduction to the topic. It then proceeds to discuss the research methodology and related work in Section 2, providing insights into the research approach and reviewing existing literature. Section 3 elaborates on the characteristics and features of blockchain technology, while Section 4 summarizes how blockchain can enhance security in IoT applications. The integration of blockchain with IoT is thoroughly explored in Section 5, which highlights the requirements and development of this integration. Moving forward, Section 6 explains the challenges and potential security threats associated with integrating blockchain technology into IoT systems. Section 7 offers a discussion on countermeasures against attacks, blockchain privacy, IoT trust issues, and solutions based on blockchain technology for IoT, including consensus algorithms. Section 8 provides a taxonomy of security research involving IoT and blockchain, concluding with research directions and open issues. Finally, Section 9 concludes the paper, wrapping up the main discoveries and implications discussed throughout the paper. The organization and layout of the paper are visualized in Figure 1.

1.3. Related Work

Various surveys have examined the integration of blockchain and IoT, primarily focusing on security aspects. In this section, several previous surveys are discussed and categorized into three groups [3,11,21,25,26,29–43]. To provide clarity, this paper categorizes prior surveys into the following distinct groups:

- Technical Surveys on Blockchain for IoT Security: These papers focus on protocol-level security[30] and architectural improvements for IoT applications.
- Comparative Studies on Blockchain Protocols: These studies analyze the performance and limitations of various protocols in blockchain and IoT applications [31–34].
- Privacy Protection Techniques with IoT and Blockchain Applications: These surveys examine blockchain's security features for applications in business, education, IoT, finance, and other fields, and also explore cutting-edge innovations such as AI-driven IoT–blockchain integration and their potential applications [30].

This categorization can aid in understanding the different focus areas within the IoT–blockchain literature and highlights this paper's comprehensive coverage across categories.

One survey [11] highlights the use of blockchain for security authentication and maintenance through decentralization, suggesting its incorporation into the IoT frameworks. Furthermore, the use of blockchain technology as a solution to address privacy and security threats has emerged due to the widespread use of IoT devices that offer the mentioned features. The above article recommends integrating blockchain into the IoT framework for an efficient and secure system to prevent negative impacts on various aspects of our environment and society. Other surveys discuss communication protocols and the relationship between IoT and blockchain, including fog and cloud computing applications [35]. Other research has addressed blockchain applications that can help to improve or create a better system for the Internet of Things; for instance, [26] addresses ways of optimizing blockchain for IoT, while [36] is focused on consensus algorithms, architecture, cryptography, etc.

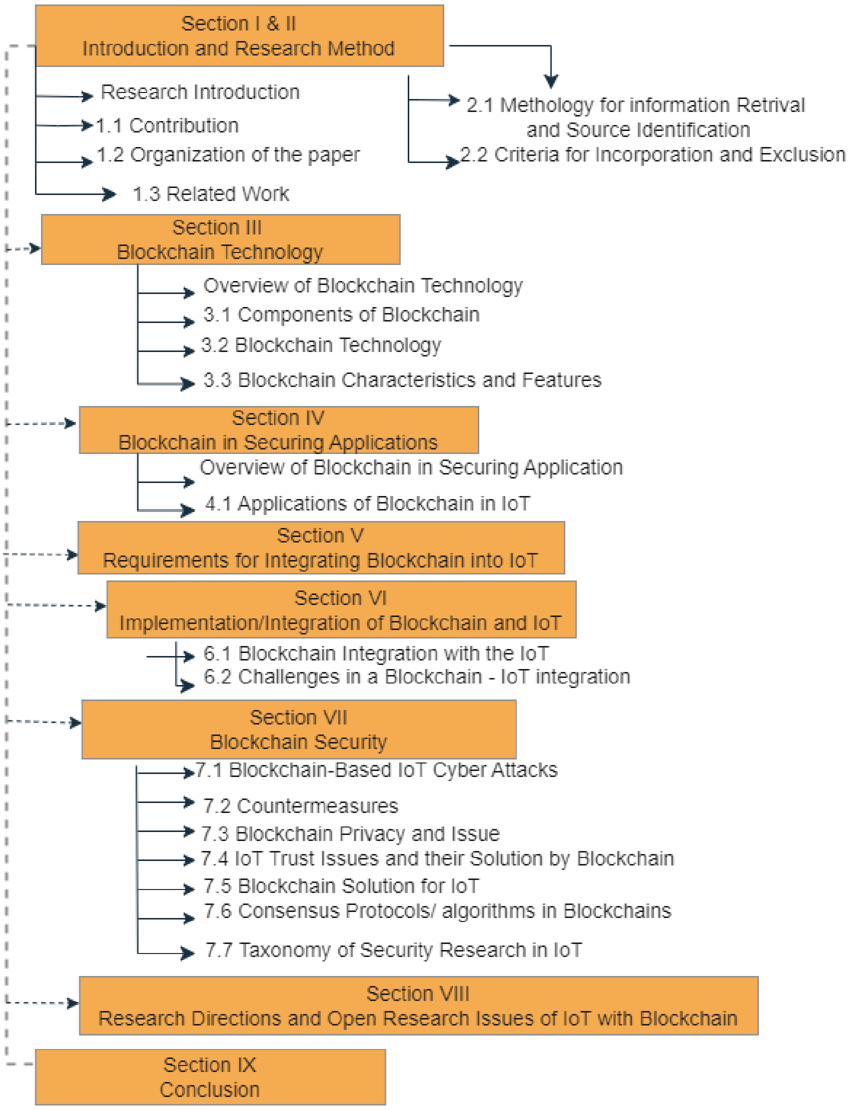
Section I & II
Introduction and Research Method
Research Introduction
1.1 Contribution
1.2 Organization of the paper
1.3 Related Work
2.1 Methology for information Retrival and Source Identification
2.2 Criteria for Incorporation and Exclusion
Section III
Blockchain Technology
Overview of Blockchain Technology
3.1 Components of Blockchain
3.2 Blockchain Technology
3.3 Blockchain Characteristics and Features
Section IV
Blockchain in Securing Applications
Overview of Blockchain in Securing Application
4.1 Applications of Blockchain in IoT
Section V
Requirements for Integrating Blockchain into IoT
Section VI
Implementation/Integration of Blockchain and IoT
6.1 Blockchain Integration with the IoT
6.2 Challenges in a Blockchain - IoT integration
Section VII
Blockchain Security
7.1 Blockchain-Based IoT Cyber Attacks
7.2 Countermeasures
7.3 Blockchain Privacy and Issue
7.4 IoT Trust Issues and their Solution by Blockchain
7.5 Blockchain Solution for IoT
7.6 Consensus Protocols/ algorithms in Blockchains
7.7 Taxonomy of Security Research in IoT
Section VIII
Research Directions and Open Research Issues of IoT with Blockchain
Section IX
Conclusion

Figure 1. Paper organization.

In addition, [32] is concerned mainly with Internet of Things security issues. The authors explored how blockchain can enhance these issues. Other surveys have reviewed blockchain-enabled IoT applications from two main perspectives, namely, data management and things management [37,38]. Advances in blockchain technology and its impact on the future of IoT applications have drawn the attention of many researchers, primarily as relates to security [39]. Other authors are interested in integrating blockchain into IoT, as this is considered a promising area of study. In [33], the authors reviewed security issues around the use of blockchain for IoT applications [40]. Finally, because Blockchain is a broad field of study, many researchers are working on theoretical aspects of blockchain such as edge computing, summarizing integration methodologies, and applications of blockchain for IoT viewed from a system design perspective [40–42].

Another paper [43] focuses on the connection between blockchain and cybersecurity. This article shows that the research on blockchain applications for cybersecurity purposes is divided into multiple domains. The authors demonstrate that over half of the literature is focused on the use of blockchain to secure domains for the Internet and IoT. Taylor [43] reviews the use of different blockchain systems such as Ethereum in developing cybersecurity solutions for IoT devices. In [21], the special difficulties and remedies related to protecting blockchain-based Internet of Things systems are considered, emphasizing the use of anonymous auditing to strengthen security and privacy while preserving the integrity and openness of blockchain transactions. The authors suggest a brand-new architecture that blends cutting-edge security mechanisms designed for Internet of Things scenarios with the decentralized nature of blockchain technology. As mentioned, security and blockchain are the areas that most researchers focus on. Furthermore, other authors provide more details about layered taxonomy, the characterization of IoT security issues, and the different countermeasures that can be taken. The authors of [36] also discuss and analyze the characteristics of blockchain security solutions and their effectiveness in securing IoT.

Various researchers have also emphasized the potential of blockchain in IoT security and its role in addressing security issues. The main solution is rooted in smart contracts as the first step in ensuring security, which is discussed in more depth in the review of blockchain-based applications in different domains by F. Casino [25]. This classifies blockchain-based applications in various domains, from the supply chain to the Internet of Things, including the limitations of blockchain and how it can be adopted in the reviewed domains.

The above literature review reveals several efforts to enhance IoT security through blockchain. However, many studies lack an in-depth analysis of specific integration challenges, particularly in terms of scalability and resource management. Most of the above surveys lack protocol comparison, do not focus on resource limits, and lack discussion of consensus mechanisms. By focusing on the limitations of blockchain for IoT in resource-constrained environments, this survey provides a unique contribution to the field in terms of detailed protocol analysis, performance evaluation constraints, and an in-depth look at consensus mechanisms in the IoT context.

This paper makes a distinctive contribution to the field by presenting a comprehensive taxonomy of security and integration challenges specific to IoT–blockchain systems. Unlike prior studies, which have primarily addressed blockchain and IoT in isolation, this survey focuses on practical considerations for integrating these technologies. Although previous research has contributed significantly to our understanding of blockchain's security potential, this survey expands the scope by evaluating specific integration methods and consensus mechanisms tailored for the IoT context. Our unique analysis of consensus mechanisms tailored for the resource constraints of the Internet of Things (IoT) adds depth to the current literature. We believe that the insights provided here will serve as a valuable foundation for both academic research and practical applications aimed at improving security in IoT environments, and could additionally drive future developments in IoT security.

2. Research Methodology

This study adopts the PRISMA framework to guide our literature review process, ensuring a systematic and transparent approach to identifying and evaluating relevant sources. PRISMA was chosen for its structured methodology, which allows for a thorough analysis of the large volume of research on IoT and blockchain. While other methodologies were considered, PRISMA's rigor in managing complex literature screening and categorization makes it particularly suitable for a survey of this scope.

2.1. Methodology for Information Retrieval and Source Identification

The research methodology for securing IoT devices through the integration of blockchain technology was designed to ensure a robust and thorough investigation. The methodology of PRISMA (preferred reporting elements for systematic reviews and meta-analysis) was adopted as the foundation of our approach. PRISMA is widely considered a gold standard framework for conducting systematic reviews, providing a structured and transparent process for identifying, evaluating, and synthesizing relevant studies [44]. To begin the research, a meticulous search process was undertaken across a diverse array of scientific databases, including Science Direct, Google Scholar, IEEE, and ACM. This expansive search strategy allowed us to cast a wide net and gather a comprehensive selection of scholarly articles about IoT security and blockchain integration. Temporal limitations on the search were avoided, resulting in the capture of relevant literature spanning the period from 2019 to 2024 [45].

2.2. Criteria for Incorporation and Exclusion

Keyword selection is a crucial aspect of a search strategy. We employed a carefully considered set of keywords, including ’IoT security’, ’blockchain integration’, cybersecurity’, ’smart devices’, and ’distributed ledger technology’. These keywords were chosen to encapsulate the core themes and concepts relevant to the research inquiry. The identification process returned a total of 925,573 results. Titles identified during the search process were subjected to screening based on established criteria outlined in the PRISMA checklist. Duplicate articles were removed using EndNote 21.1 reference management software. Articles that met the screening criteria proceeded to title and abstract screening, resulting in the exclusion of 17,590 articles. The study was meticulously structured and executed following scoping and systematic review guidelines and was guided by the PCC (Population, Context, and Concept) framework. This framework offers a systematic method for crafting research questions and identifying relevant study components, ensuring that the analysis is comprehensive and extensive. In implementing the search strategy, the titles and abstracts of the retrieved articles were rigorously screened based on the predefined criteria established in the PRISMA checklist, which equated to 17,890 articles. Duplicate articles were identified and removed using reference management software to streamline the screening process. Ultimately, 168,270 articles that met the screening criteria were submitted for full-text evaluation.

During the full-text assessment, each article underwent a detailed full-text evaluation for relevance, duplication, and availability. Only English-language papers meeting the inclusion criteria were considered for further analysis. Journal-wise statistics were analyzed to acquire insights into the distribution of the relevant literature across different publication sources, adding valuable context to the findings. In addition to the systematic review, a comprehensive analysis of the existing literature was conducted to identify relevant studies on IoT security, blockchain integration, and related domains. This synthesis offers a holistic evaluation of the application of blockchain technology in securing IoT devices. Exclusion criteria were used to guarantee the integrity and focus of the analysis. Articles containing duplicated information, irrelevant content, or subject matter not directly related to IoT security and blockchain integration were excluded from consideration. The number of studies excluded on this basis amounted to 148,450 articles. In addition, resources such as case series, reports, brief communications, and editorial comments were omitted from the final selection of articles to preserve the scholarly rigor of the study. This comprehensive and methodical approach aimed to achieve a distinctive understanding of the integration of blockchain technology for securing IoT devices. Keeping in mind established methodologies and guidelines, the objective was to produce research outcomes that are rigorous, reliable, and actionable (Figure 2).

The literature screening adhered to PRISMA guidelines, ensuring a structured approach to source selection and analysis. Criteria included relevance to IoT security and integration, publication date, and resource constraints in IoT settings. The discussion connects these findings to real-world IoT applications, emphasizing blockchain’s role in enhancing data security and privacy across sectors such as healthcare, supply chains, and smart cities.

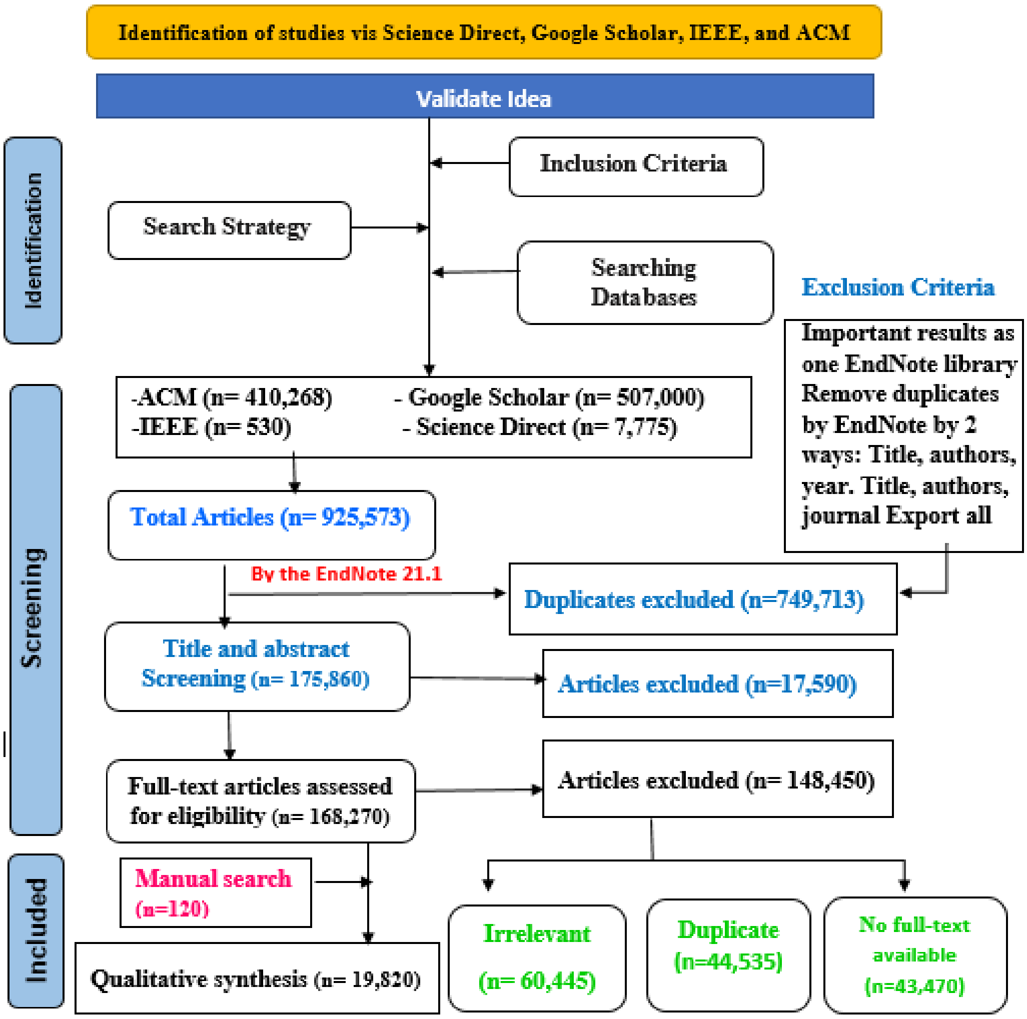
Identification of studies vis Science Direct, Google Scholar, IEEE, and ACM
Validate Idea
Identification
Inclusion Criteria
Search Strategy
Searching Databases
Exclusion Criteria
Important results as one EndNote library Remove duplicates by EndNote by 2 ways: Title, authors, year. Title, authors, journal Export all
Screening
-ACM (n= 410,268)
-IEEE (n= 530)
- Google Scholar (n= 507,000)
- Science Direct (n= 7,775)
Total Articles (n= 925,573)
By the EndNote 21.1
Duplicates excluded (n=749,713)
Title and abstract Screening (n= 175,860)
Articles excluded (n=17,590)
Full-text articles assessed for eligibility (n= 168,270)
Articles excluded (n= 148,450)
Included
Manual search (n=120)
Qualitative synthesis (n= 19,820)
Irrelevant (n= 60,445)
Duplicate (n=44,535)
No full-text available (n=43,470)

Figure 2. The PRISMA model that guided the article selection process.

3. Blockchain Technology

Satoshi Nakamoto, who anonymously created Bitcoin, is credited with first presenting the idea of a blockchain. Often, people mistake blockchain for Bitcoin [38]. Bitcoin is a digital currency based on blockchain technology that permits trading freely worldwide without requiring a financial institution as a guarantor. However, Bitcoin is merely a monetary application of blockchain technology. Blockchain is characterized as an unchanging auditable timestamp and tamper-resistant block ledger that shares, stores, and uses information in a peer-to-peer (P2P) way [36,45–47]. Figure 3 shows the types of decentralized ledger technology, categorized into data structure ledgers and permission and accessibility ledgers.

The data stored in a blockchain can vary; examples include payment histories and personal information. Blockchains store information in blocks, which are then connected in a chain. When new information is added, it is placed into a new block; once filled, the new block is secured to the previous block, maintaining the information in sequential order [44–46,48,49]. Figure 4 depicts types of blockchain networks, including structured networks, unstructured networks, and hybrid networks.

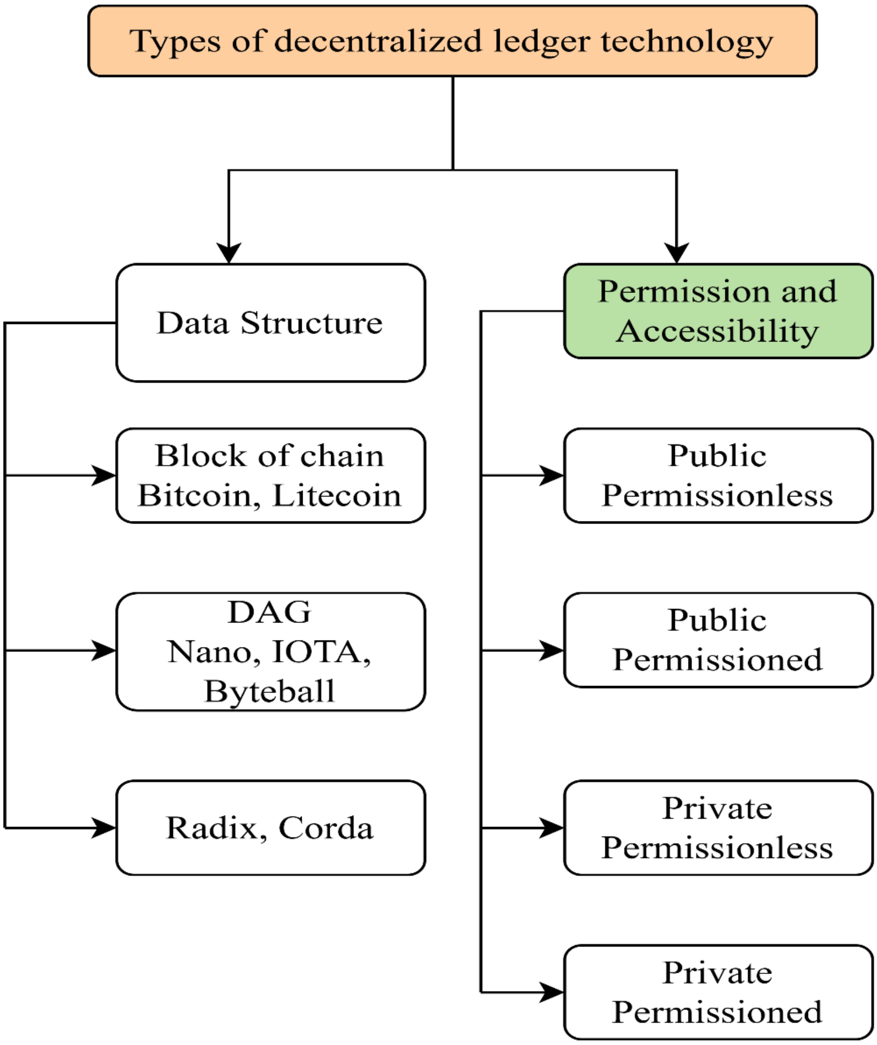

Figure 3. Types of decentralized ledger technology.

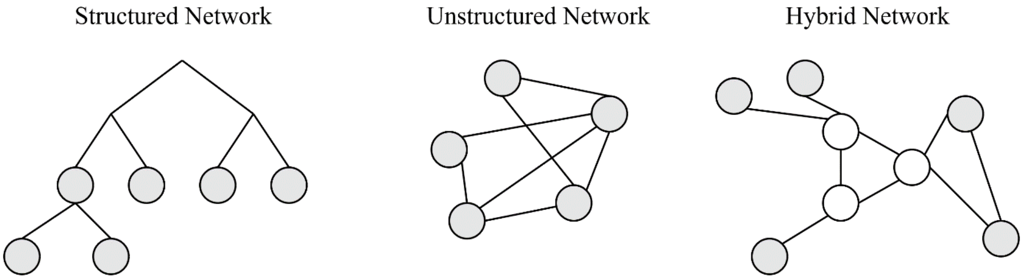

Figure 4. Blockchain network structures.

3.1. Components of Blockchain

Blockchain technology can convey several benefits over today's arrangements, and these components make blockchain technology different from other technologies used to date. There are several elementary features of blockchain technology: ledger, block, minor, hashing, consensus mechanism, and transaction [46,50,51]. The primary elements of blockchains are shown in Figure 5.

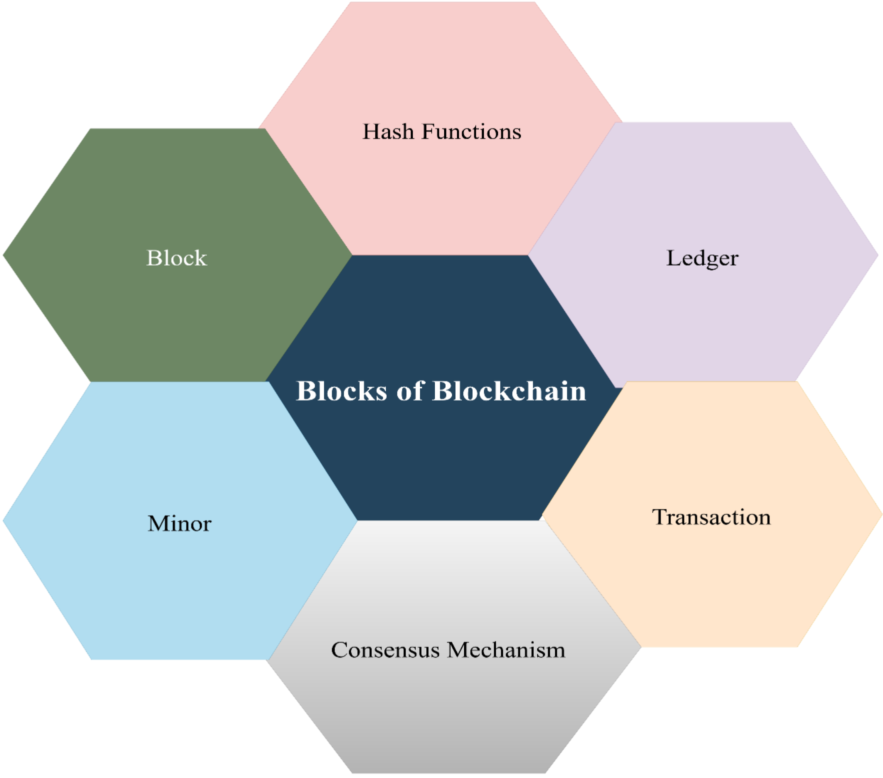

Figure 5. Main components of a blockchain.

Ledger: The ledger is a data structure that can store various types of information [46,50]. Although it functions similarly to a traditional database, it possesses unique features. In contrast to databases, which most often structure data into tables with rows and columns, and utilize a relational model for queries and information retrieval from multiple sources [52–54], a ledger captures and logs each transaction ever made by network users, both historical and current. The ledger is distributed among all nodes within the network, ensuring that every participant maintains a copy [39,46,50,52].

Block: A block is composed of a set of transactions, and is connected to the preceding block through its hash value to create a series of linked blocks [38,52]. Every block is assigned a distinctive hash, which is essential for validating the content by preserving data integrity [46,53,55]. The hashing function is resistant to collisions, indicating that it is highly improbable for different datasets to produce identical hashes, which is crucial for establishing and confirming the hash values of the blocks [46,52,54].

Transaction: A transaction represents the fundamental processing unit, made up of various transactions between participants that are subsequently grouped into a block [38,44,54]. For a transaction to be included in a block, approval from a majority of network nodes is required [56]. The size of the transaction influences miners, as smaller transactions need fewer resources and are easier to verify compared to larger ones. Miners are computers or entities responsible for resolving mathematical problems, mainly involving hash functions, to generate new blocks [38,44,46,52].

3.2. Blockchain Technologies

Blockchain technology consists of a distributed decentralized ledger that operates in a trustless environment [50,56]. It first became popular with the development of applications such as Bitcoin. Years later, Ethereum emerged as the second-most popular cryptocurrency and application of blockchain technology. Numerous research articles [48,50,56] have pointed out that blockchain technology is based on different layers. The primary layers of blockchain technology include the data, application, consensus, and network layers.

- Data Layer: This layer consists of transactions based on a hash function, block, Merkle tree, and digital signature [33,55]. The data block is divided into two parts consisting of transaction records organized into a Merkle tree, which is a binary tree structure that summarizes and securely checks content within a large dataset [33,50] Figure 6 illustrates the structure of a Merkle tree.

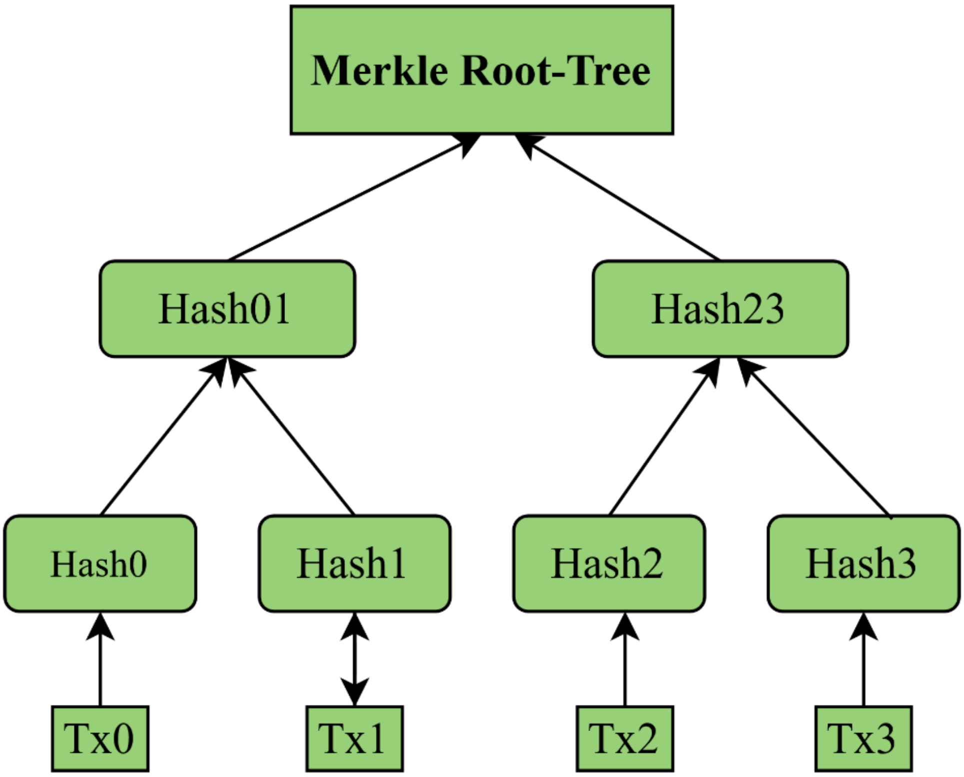

Figure 6. Merkle tree structure.

- Merkle trees are generated by hashing nodes in a kind of for-loop function until one hash is left, called the root hash. The final component of the data layer is the digital signature, which is authenticated digital content that guarantees the integrity of the transaction [33,47,48,50]. It is sometimes complicated to understand the architecture of IoT with blockchain. Figure 7 visualizes the IoT and blockchain architectures in different layers and shows the characteristics of each layer; the bottom of the figure shows the IoT and blockchain layers and their respective functions in the network.
- Application Layer: This layer is used for smart contracts, dApps, and chain code, and includes the presentation layer (scripts, user interface, APIs) and execution layer (smart contracts, chain code). Each transaction in the chain is run from the execution layer, which follows instructions given by the presentation layer [48,57]; see Figure 7.
- Consensus Layer: This layer serves a crucial function in maintaining the reliability of the blockchain platform [50]. A consensus is a set of rules enforced by this layer that each participant must follow to ensure a smooth generation process for guaranteeing the validity of transactions/blocks [48,57,58]. There are different kinds of consensus for guaranteeing blockchain consistency, including probabilistic and deterministic methodologies. This layer ensures the reliability of the blockchain platform. Consensus rules enforced in this layer guarantee smoother transaction and block generation and validation [48,50,57]. Consensus methods include probabilistic and deterministic methodologies [48,50,57].
- Network Layer: This layer establishes communication between nodes, also known as a peer-to-peer network (P2P), ensuring that all nodes are connected, which is

necessary to propagate blocks through the network and synchronize the valid state of the blockchain. Figure 8 illustrates a P2P network architecture using six nodes.

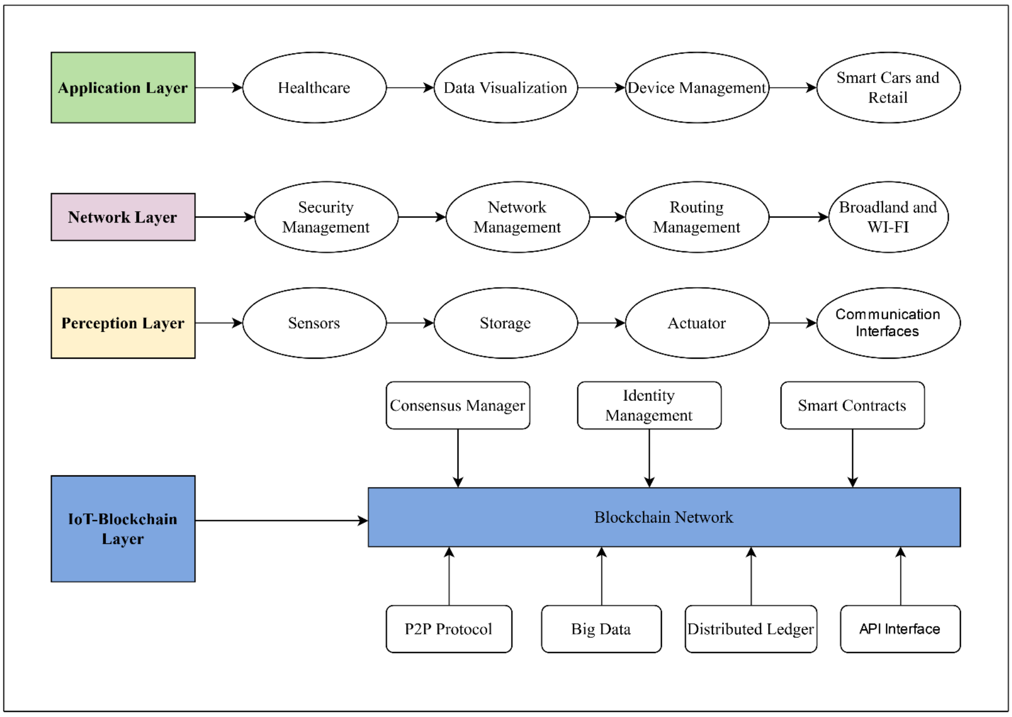

Figure 7. Architecture of IoT with blockchain.

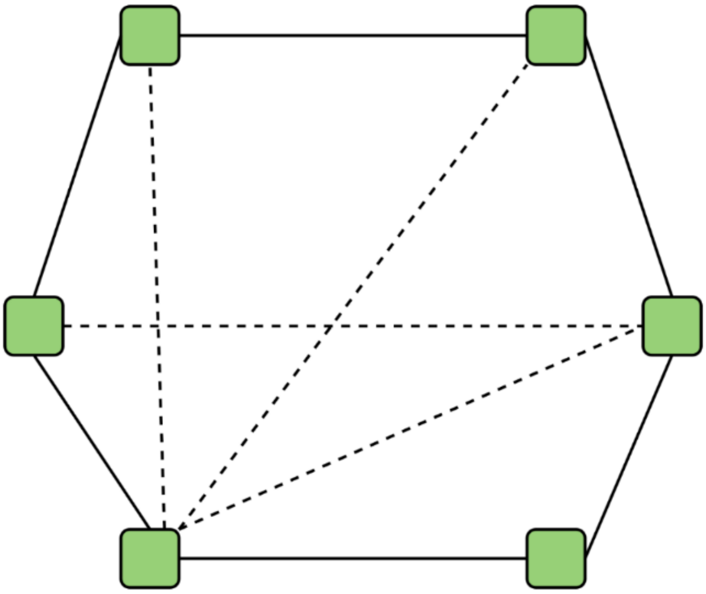

Figure 8. Architecture of a peer-to-peer network with six nodes.

This network can be defined as a network of computers where the computers or nodes are shared and the workload of the network is also been shared with other nodes to achieve the final nodes of the blockchain which processes transactions and blocks [48,50,57,58]. The nodes distributed in this layer are light nodes that store only a header or keys of the blockchain and send transactions to the other nodes, called full nodes, which check and validate transactions and then store the finished distributed ledger. Table 1 provides an overview of the use of nodes for storing and validating transactions.

Table 1. Types of nodes in a blockchain network.

Nodes	Full Node	Light Node	Transaction Issue
Storage	Full Blockchain	Block Headers	None
Validator	Yes	No	No

3.2.1. Blockchain Tokenization: A Digital Transformation

Figure 9 illustrates a fundamental concept in the evolving landscape of digital assets, namely, blockchain tokenization, which is the process of converting real-world assets into digital tokens on a blockchain network.

3.2.2. Key Components of Blockchain Tokenization

There are two key components of blockchain tokenization which categorize assets of value into tangible and intangible assets based on their properties. Further details are provided in the upcoming sections.

- Tangible Assets: Examples of these valuable physical assets include gold, real estate, and art. Utilizing blockchains to tokenize these assets provides benefits such as better liquidity, greater transparency, diminished fraud risk, and enhanced accessibility.
- Intangible Assets: Examples include intellectual property, voting rights, and licensing agreements. Tokenization facilitates royalty management, ownership transfer fractional ownership, regulatory compliance, and liquidity.
- Tokenization offers a range of services, such as facilitating royalty management and distribution, streamlining the ownership and transfer processes, and enabling fractional ownership of intellectual property. It can also democratize investments by allowing for smaller investments, improving regulatory compliance through transparent recordkeeping, and enhancing liquidity for previously illiquid assets. There are several different types of tokenization categories available, catering to different domains such as security. Tokens which represent ownership stakes in a company or asset are akin to traditional securities. Cryptocurrency and tokenization encompass two primary types of token, namely, currency tokens and utility tokens (see Figure 9). Utility tokens offer access to a product or service, usually on a specific blockchain network, and function similarly to loyalty points or vouchers, while currency tokens serve as a medium of exchange within a specific ecosystem. These tokens have huge implications for a wide range of sectors, as they can help to increase liquidity, improve transaction efficiency, and enhance the transparency and provability of assets.
- Fungible tokens are based on the ERC-20 standard, which means that they are identical and interchangeable, similar to traditional fiat currencies. Nonfungible tokens (NFTs) are based on the ERC-721 standard and represent unique assets with distinct properties, such as digital art or collectibles. The main quality of ERC721 tokens is that many tokens can be maintained by a single smart contract, unlike ERC20 tokens, for which one smart contract is required for each token. Examples of NFTs include Ethereum's Cryptokitties and the digital art and collectibles available for purchase on NFT marketplaces such as Nifty Gateway, OpenSea, and NBA Top Shot.

Blockchain tokenization offers benefits in terms of increased liquidity and accessibility for various assets. Transparency and security are enhanced through immutable blockchain records that cannot be tampered with or changed once posted on the blockchain network. Fractional ownership opportunities for investors can be vital in the case of tangible asset ownership. Streamlined processes for asset management and transfer may consider currency tokens, while there is huge potential for new business models and financial instruments (see Figure 9).

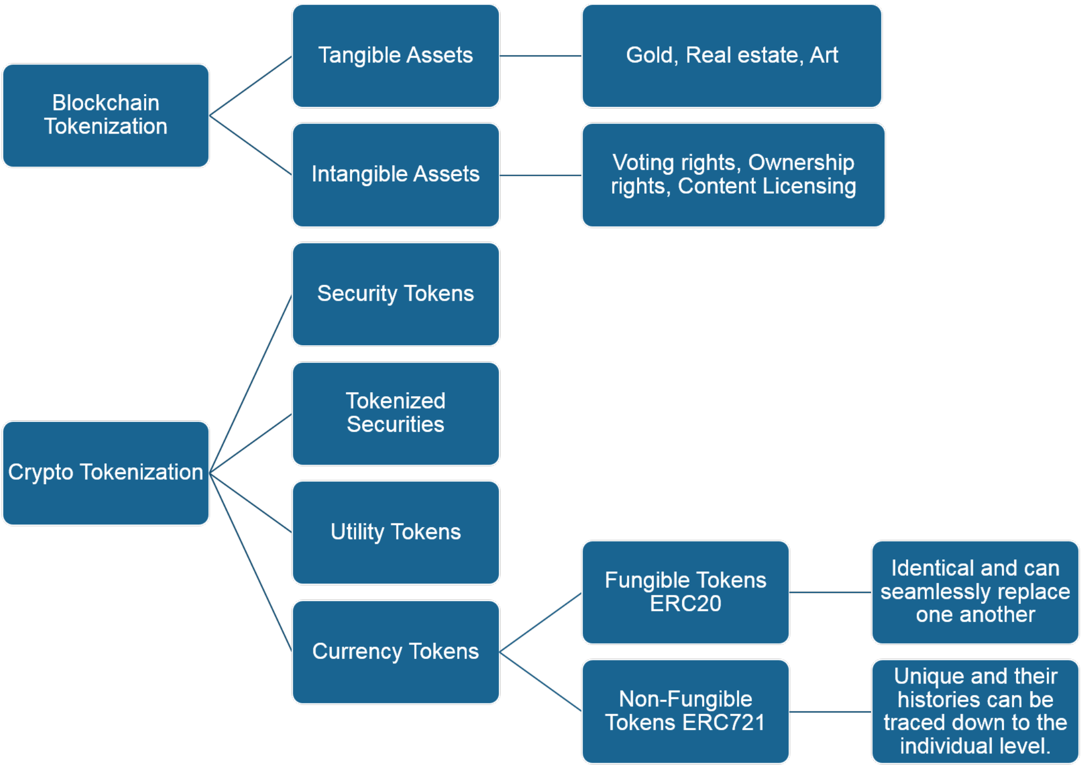
Blockchain Tokenization
Tangible Assets
Gold, Real estate, Art
Intangible Assets
Voting rights, Ownership rights, Content Licensing
Crypto Tokenization
Security Tokens
Tokenized Securities
Utility Tokens
Currency Tokens
Fungible Tokens ERC20
Identical and can seamlessly replace one another
Non-Fungible Tokens ERC721
Unique and their histories can be traced down to the individual level.

Figure 9. Blockchain tokenization for assets over a blockchain network.

3.3. Blockchain Characteristics and Features

Blockchain technology has a robust structure, with valuable characteristics such as decentralization, immutability, identity, nonrepudiation, transparency, traceability, pseudonymity, anonymity, and security; Figure 10 highlights these features.

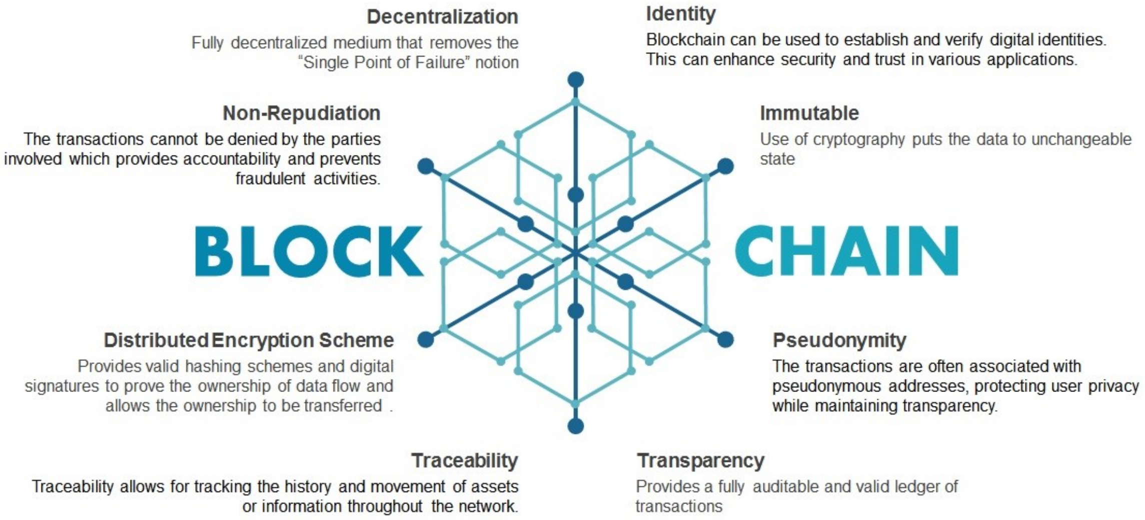
Decentralization
Fully decentralized medium that removes the "Single Point of Failure" notion
Identity
Blockchain can be used to establish and verify digital identities. This can enhance security and trust in various applications.
Non-Repudiation
The transactions cannot be denied by the parties involved which provides accountability and prevents fraudulent activities.
Immutable
Use of cryptography puts the data to unchangeable state
BLOCK
CHAIN
Distributed Encryption Scheme
Provides valid hashing schemes and digital signatures to prove the ownership of data flow and allows the ownership to be transferred .
Pseudonymity
The transactions are often associated with pseudonymous addresses, protecting user privacy while maintaining transparency.
Traceability
Traceability allows for tracking the history and movement of assets or information throughout the network.
Transparency
Provides a fully auditable and valid ledger of transactions

Figure 10. Salient features of blockchain technology.

1. Decentralization: This is among the most characteristic features of blockchains, which consist of a decentralized and distributed environment established through P2P communication between nodes, as shown in Figure 10 [59]. Decentralization utilizes all users' processing power, thereby decreasing latency and risk of single-point failures [39,46,47,51]. Network participants can access all data records without needing a central controlling authority [33,55].

2. Immutability: As illustrated in Figure 10, one of the primary attributes of blockchain technology is its capacity to preserve transaction integrity via immutable ledgers [51]. In contrast to a central authority, where a single organization oversees data integrity, blockchain utilizes collision-resistant hash functions to connect each block to its predecessor, thereby affirming the integrity of the block's content [33,47]. An additional facet of immutability is that modifications to the ledger's blocks cannot occur without the consensus of all users [39,46,47,51]. Moreover, blockchain safeguards data integrity through collision-resistant hash functions, rendering blocks unchangeable without user consent.
3. Identity: The ownership of an Internet of Things device may shift throughout its life cycle, necessitating an identity management system that is both efficient and secure. Many of the characteristics associated with Internet of Things devices, such as the manufacturer, GPS coordinates, serial number, and type of device, require an administrator that is trustworthy and secure [54] In every phase of the life of Internet of Things devices, blockchain has the potential to present a viable solution that may help to reduce the aforementioned issues. Through its use of decentralized and distributed ledgers, blockchain technology can offer approved and trustworthy identity management of linked Internet of Things devices together with information on their intricate qualities and relationships. This makes it possible to monitor every lifecycle stage of an Internet of Things device, from the manufacturer to the supplier and ultimately to the customers [56]. Overall, blockchains can provide secure identity management for IoT devices throughout their lifecycle.
4. Non-Repudiation: the process of validation uses private keys to sign transactions, which helps to confirm other participants with the equivalent public key. Therefore, each signed transaction cannot be refused by the transaction originator [33,46,47]. Furthermore, blockchain uses a private key for transaction validation, confirming participant authenticity. See Table 2 for more details about decentralized and centralized systems and their features.

Table 2. Comparison of centralized and decentralized systems.

Features	Decentralized	Centralized
Transaction Mode	Decentralization	Centralization
Resource Consuming	Low	NHigh
Transaction Cost	Low	High
Flexibility	Not Supervised	Supervised
Data Privacy	High	Low
Data Storage	Decentralized ledger	Centralized Database
Information Transparency	High	Low
Cost	Low	High

5. Transparency: All of the data encapsulated in a block can be viewed by all participants in the blockchain, which means that every user can access and interact with the blockchain network and all users have equal rights [46,47,51,56]. Overall, blockchain allows all participants to view the data encapsulated in blocks.
6. Traceability: All the transactions saved in the blockchain have a timestamp attached which is recorded when the transaction is executed. This allows each user to quickly verify and trace the origins of historical data items after analyzing the blockchain data with current timestamps. This enables users to trace back to the original transaction [47,51]. Furthermore, blockchains record timestamps for each transaction, enabling users to trace the origins of data.

7. Pseudonymity: Each transaction in a blockchain uses a certain level of privacy by making blockchain addresses anonymous [47]. Blockchain information can help to identify scams and illegal transactions that may appear [33,47]. However, blockchain can only provide a certain level of privacy, as blockchain addresses are traceable. Overall, blockchain maintains privacy by making blockchain addresses anonymous.
8. Anonymity: Each node in the blockchain engages with the network using its public key, which allows it to be addressed across the network while the true identities remain unknown [55]. It is important to note that blockchain does not offer adequate confidentiality protection owing to certain significant limitations [47,55]. In essence, blockchain employs public keys for network engagement without disclosing actual identities.
9. Security: A key advantage of blockchain technology is its enhanced safeguarding compared to existing solutions [55,56]. Blockchain establishes a secure environment resistant to attacks through public key infrastructure. Additionally, the consensus mechanism provides a reliable method that bolsters the security of the blockchain [26,46,47]. In summary, blockchain enhances protection through the implementation of public key infrastructure and consensus mechanisms.

4. Blockchain for Securing Applications

Blockchain technology has gained a great deal of attention due to features of its decentralized architecture such as security, anonymity, centralization, and traceability [26]. The progression of blockchain technology from its inception in 2008 to its anticipated future in 2030 highlights key milestones, influential figures, and emerging trends within the blockchain ecosystem. Blockchain 1.0 was introduced by Satoshi Nakamoto in the year 2008 to support the concept of Bitcoin, described in a white paper as a peer-to-peer electronic cash system focused on decentralized transactions without a central authority. The idea led to further implementation in operational form, which gave birth to Blockchain 2.0, starting with Bitcoin's core component being implemented as a public ledger for all transactions in the year 2009 and lasting until the year 2011. This era established the foundation for blockchain as a technology beyond cryptocurrency.

Vitalik Buterin later proposed the Ethereum platform in 2013, which expanded the potential of blockchain technology. This is referred to as Blockchain 3.0, which enabled the creation of decentralized applications (dApps) and smart contracts. His innovation laid the groundwork for various industries to adopt blockchain technology. In 2018, Blockchain 4.0 focused on distributed ledger technology and its applications in industries such as finance, supply chain, and healthcare. The emphasis on interoperability, cloud node access, and middleware for seamless integration kicked off the integration of decentralized ledger technology in domains apart from cryptocurrency.

With the emergence of the visionary stage after 2021, technology encompassing the metaverse, industrial infrastructure, and a robust blockchain ecosystem has led to Blockchain 5.0, which focuses on advancements in identity and access control, trust mechanisms, and communication technology, including anticipating and adapting to the security and privacy concerns of future eras. The timeline depicted in Figure 11 highlights the increasing complexity and sophistication of blockchain technology over time. Each stage builds on the previous one, demonstrating the evolutionary nature of blockchain development. The involvement of key figures such as Satoshi Nakamoto and Vitalik Buterin underscores the importance of individual contributions to the field [26,45,51]. Blockchain ensures enhanced security through the utilization of public keys, significantly bolstering protection against potential threats. All interactions between devices are cryptographically secured via technology [33,46]. The cryptographic framework of blockchain relies on hashing each block while incorporating it into the previous one. This block-hashing process forms a virtual chain linking them together, thereby earning the name blockchain [26,45,46,51].

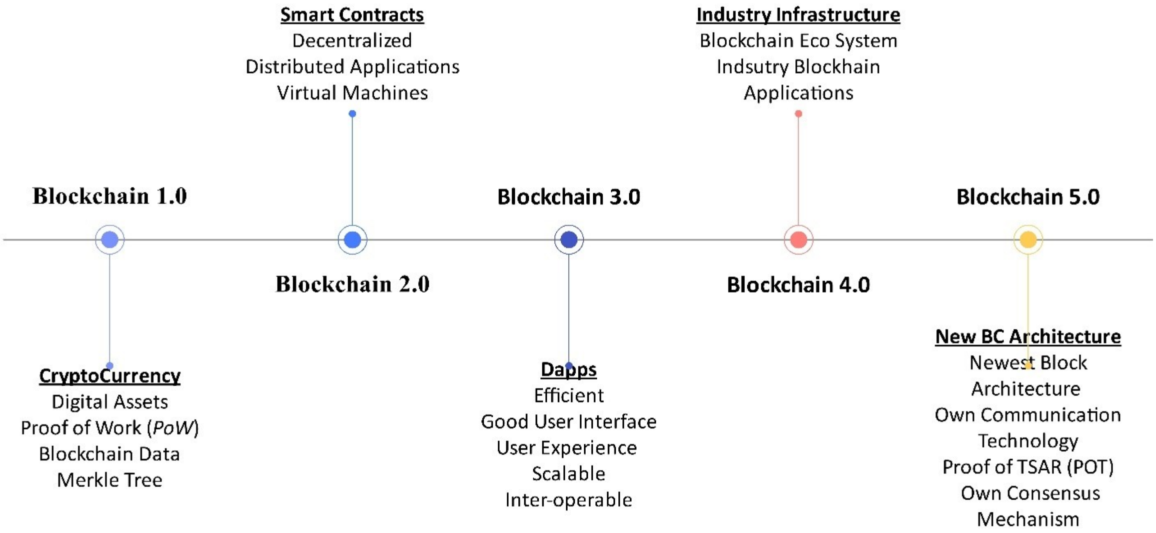

Figure 11. Development of blockchain.

Blockchain technology can also enhance low-level security, improving remote attestation; this process verifies whether a device's trusted computer base (TCB) can be trusted. Different proposed blockchain–IoT applications are related to smart cities and industrial processes. These frameworks securely integrate intelligent devices and applications to provide smart city applications [26,33,60]. Blockchain can be used in securing applications connected to IoT networks that are intended to address existing technologies. Blockchains can confirm the stored data in the network against all kinds of attacks and provide a secure platform for all devices within the same network through which they can communicate with each other without the need for a central server [39,46,56,61,62].

Today, it can be seen that blockchain is being used in many applications, as blockchain technology can improve and help all applications, especially IoT [36,59]. Blockchain plays a fundamental key in preserving confidentiality when using different applications. This confidentiality is managed by the user key, which would be impossible for an attacker to steal. This excellent management system frees users from managing their encrypted keys. Using the key makes the user feel safer from attacks, as the blockchain offers better security when using applications [26,36,39,59]. Another essential feature in securing applications consists of transactions and digital signatures. Transactions in a blockchain network require a public-private key pair. Peers use their private keys to sign transactions and then use the recipient's blockchain address to deliver them. One example of this is Bitcoin transactions, which use SHA-256 encryption for user addresses [51,58,61]. Two different blockchains can be connected through a process called side-chaining. A sidechain can be defined as a synchronized blockchain running in parallel with an existing blockchain, which is called the main chain [60,63]. Security and privacy are crucial parts of developing applications. Where IoT devices use blockchain-based privacy and security, it is essential to the entire network and platform [64].

Blockchain is a promising solution when it comes to security applications, as applications with blockchain can enable a much higher security level than other technologies available to date [60,64,65]. Among the ideas that have been presented [36,65] are blockchain solutions for securing applications based on IoT device control and configuration supported by Ethereum. It is important to remember that devices need to support these applications. In this case, the private key should be stored on the device and the public key should be registered as a regular transaction on the Ethereum blockchain. When this enables access, the application on the device can be accessed through ethernet while using its public key. This proposed approach for using IoT has proved that these features and security can be introduced using blockchain [36,61,63–65]. Similarly to IoT systems, blockchain solves problems in securing applications. The structure of a cryptographic blockchain is based on hashing each block attached to another block, which is promising for the future.

Blockchain technology improves and secures applications with the help of encryption; lately, digital signatures have brought blockchain to the market because security is a primary concern for IoT and applications [33,60,63]. Establishing a wireless network is increasing in the industrial environment, causing an increase in the measurability and increased chances of wireless communications in the organization [47]. Open wireless channels create issues in IoT and blockchain applications due to safety violations such as jamming, overhearing, and the growth of repeat attacks. However, blockchain schemes still have security vulnerabilities such as program deficiencies of smart contracts. For the future of secure applications, blockchain nodes should be resource-constrained, as weighted encryption techniques may not be feasible in IoT [39,47,56,61].

4.1. Applications of Blockchain in IoT

There is an increasing number of applications for Blockchain in IoT. This is happening because blockchain technology can help to overcome different IoT challenges. Blockchain and the Internet of Things (IoT) are two emerging technologies that offer unique capabilities and solutions for various industries when combined, as shown in Figure 9. When IoT devices record data on a blockchain, it becomes tamper-proof. In industries where data integrity is essential, such as healthcare, supply chain, and industrial processes, a blockchain can create an immutable ledger. On the other hand, IoT devices can share data with other devices securely, and data can only be accessed or modified by authorized parties. Traditional IoT systems depend on centralized servers or cloud platforms, whereas when data can be distributed across a decentralized network using a blockchain, the risk of system failures and the need for intermediaries can both be reduced.

Blockchain technology can clarify who owns and controls the vast datasets produced by IoT devices, while users have the option of providing temporary access to their information. IoT sensors contribute data about the location, status, and origin of products to the blockchain transparently. Automated microtransactions on blockchain networks can be executed through IoT devices. For instance, a connected car can autonomously settle parking fees or pay for electricity at charging stations using blockchain-enabled micropayments. Furthermore, blockchain plays a significant role in forming and overseeing secure identities for IoT devices. This is essential to ensuring that only authorized devices exchange information or utilize specific services [26,33,48]. Conversely, the integration of blockchain with IoT results in substantial data volumes, presenting scalability challenges when these technologies are deployed on a wide scale. There are also issues concerning the latency of blockchain transactions; see Figure 12.

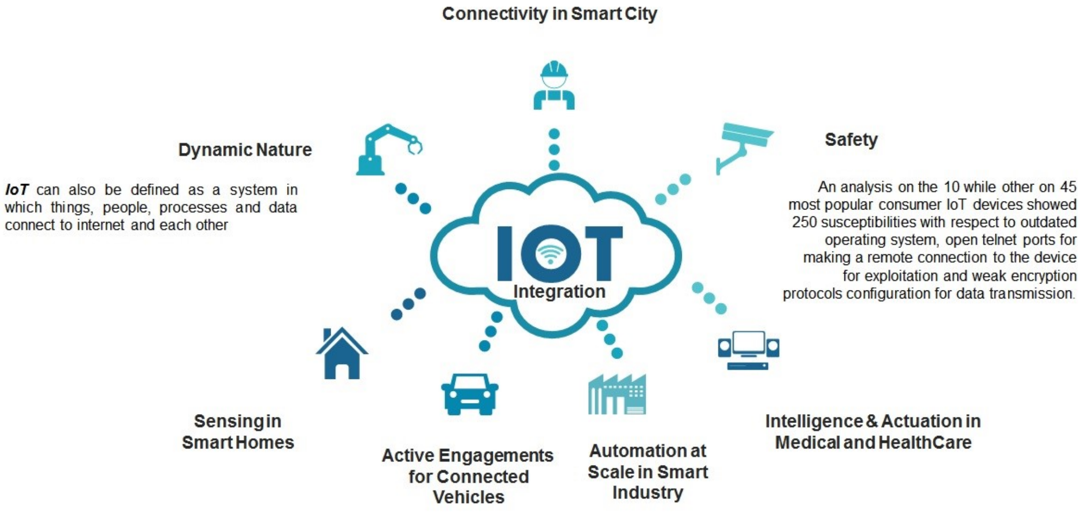
Connectivity in Smart City
Dynamic Nature
IoT can also be defined as a system in which things, people, processes and data connect to internet and each other
Safety
An analysis on the 10 while other on 45 most popular consumer IoT devices showed 250 susceptibilities with respect to outdated operating system, open telnet ports for making a remote connection to the device for exploitation and weak encryption protocols configuration for data transmission.
IOT
Integration
Sensing in Smart Homes
Active Engagements for Connected Vehicles
Automation at Scale in Smart Industry
Intelligence & Actuation in Medical and HealthCare

Figure 12. Internet of Things applications.

The convergence of IoT and blockchain in Industry 5.0 represents a transformative step toward building secure, decentralized systems that enhance human-machine collaboration, efficiency, and decision-making. Unlike Industry 4.0, which primarily focuses on automation and machine-to-machine communication, Industry 5.0 places greater emphasis on human-centric technologies that prioritize personalization, sustainability, and resilience. Blockchain, when integrated with IoT, not only addresses long-standing issues such as data security and privacy but also fosters seamless interoperability between devices, platforms, and ecosystems.

1. Smart Manufacturing
   The manufacturing industry is changing a lot and is moving from automated manufacturing to what is called smart manufacturing [25,26]. Data plays one of the most significant roles in this transmission. IoT devices augmented with blockchain can create decentralized networks that track and authenticate every stage of a product's lifecycle from sourcing raw materials to final delivery. Blockchain ensures that data are immutable and transparent, fostering trust between stakeholders. Industry 5.0 further builds on this by integrating human input into these systems, allowing workers to make informed decisions based on accurate real-time data while maintaining high levels of trust and accountability [25,26,33]. Blockchain can address the interoperability problem by connecting IoT systems using a P2P network, which allows data sharing in all industrial sectors [26,33,48]. Blockchain also helps to improve security in smart manufacturing, as most IoT systems thus far have been centralized. Automated manufacturing is often integrated with decentralized blockchain technology, which provides security and confidentiality compared to centralized systems [26,33,47,48]. Overall, blockchain can improve security and data sharing in smart manufacturing environments through decentralized systems and smart contracts.
2. Supply Chains
   A supply chain can be defined as a set of activities, components, and resources that must deliver a product or service to customers [26,33]. The final product sent across countries using different manufacturers may consist of forged components. Moreover, the need for products to pass through various manufacturing processes introduces risk [33,48]. Deploying anti-fraud technology in the supply chain can be very expensive. On the other hand, blockchain can solve this problem more affordably. Blockchain and IoT impact supply chain goals such as speed, quality, cost, risk reduction, flexibility, and more [25,26,33,47,48,66]. At base, trading consists of a lawful contract [47] between a buyer and seller, with trade achieved as the product. During the transport of goods, it is often the case that a third party checks the trading procedure [47,48]. In certain cases, the parties may need to have recourse to a regulatory entity to solve any problems or to act as a guarantor [33,47,48]. In this context, blockchain can help to improve traceability and reduce fraud in supply chains by immutably recording each step of the product lifecycle.
3. Food Industry
   The role of blockchain in the food sector primarily involves the traceability of food products to ensure food safety [47,48]. Current IoT solutions struggle to provide food traceability within the food supply chain. Numerous providers can stipulate different food-producing organizations. Therefore, a need exists to digitize materials from sources in the manufacturing sector. Blockchain technology can track food, helping to ensure its origin [26,33,47]. Different sources have claimed that there is a need for blockchain to establish a supply chain from farming to food manufacturers which guarantees data traceability in food supply chains [25,47]. Blockchain combined with food supply chain calls can allow consumers to track the total amount of food manufacturing procedures. The Colombian natural coffee industry is also using blockchain technology. In addition, there is encouragement by the Electronic Product Code to use IoT tags and blockchain, which can stop information interference and

confidentiality revelation [25,26,33,47,66]. Overall, blockchain can help to ensure food traceability and safety.

4. Healthcare
Healthcare is rapidly evolving with the integration of digital technologies which promise to revolutionize clinical data management and improve both outcomes and processes [47,48]. As one of the most pressing socioeconomic issues due to population growth [26,67,68], the healthcare sector faces significant challenges, particularly with limited hospital resources. Moreover, blockchain-enabled IoT systems can secure sensitive patient data collected through wearable devices such as heart rate monitors or glucose sensors. Beyond securing this data, blockchain's decentralized ledger facilitates interoperability by enabling different healthcare providers and IoT devices to securely access and exchange patient information. This ensures continuity of care, reduces redundancies in data collection, and enhances the patient experience, aligning perfectly with Industry 5.0's focus on personalized human-centered solutions [26,33,36]. For example, patients can now remain at home while using wearable devices that monitor metrics like heart rate and blood pressure [26,33,48]. These devices enable doctors and nurses to access healthcare data anytime and anywhere via the network. However, these data also raise concerns regarding security and privacy [26,47,48]. Blockchain technology offers a potential solution by ensuring the privacy and security of healthcare data stored on cloud servers and managing this data effectively [67,68]. Medical sensor data can be collected and transmitted automatically to the system through smart contracts, enabling real-time patient monitoring [26,33,47,48,66]. By implementing these measures, blockchain can address privacy and security issues in healthcare data management.
5. Internet of Vehicles
The Internet of Vehicles integrates vehicle-to-vehicle networks, vehicle-to-infrastructure, vehicle-to-roadside networks, and vehicle-to-pedestrian networks [33,48]. The automotive sector is leading technically superior branches by scaling from electric, hybrid, and self-driving smart cars in the Industrial Internet of Things in combination with IoT-linked cars [26,33,47]. Securing message transmission and execution are some of the challenges that come with the decentralization, heterogeneity, and trustworthiness of the Internet of Vehicles. Integration between blockchain and the Internet of Vehicles is needed to solve these challenges [25,26,47]. Blockchain technology conserves the energy and information interactions between electric and hybrid electric vehicles using a smart grid. Communication networks using Unmanned Aerial Vehicles (UAVs) to deliver product items may lack wireless communication capability and data on real-time traffic flows. Integrating blockchain technology into UAV networks can provide confidence in UAVs [25,26,33,47]. Much development of an autonomous platform based on the Ethereum blockchain is used to provide trust management on UAVs. Developers are working on developing a blockchain-based system to serve privacy and security for UAV data [33,66,69]. In general, blockchain integration can secure communication and data exchange in vehicular networks.
6. Smart Grids
In the context of renewable energy resources, it is possible to distinguish pure consumers from prosumers who generate energy instead of just consuming it [33,47]. The energy traded between consumers and prosumers is called P2P energy trading [26,47]. Blockchain–IoT integration enables decentralized management of resources such as water and electricity by reducing reliance on centralized infrastructure. Blockchain facilitates peer-to-peer energy trading systems that empower citizens to trade surplus energy, while IoT sensors ensure accurate measurement and tracking. This aligns with Industry 5.0's aim of creating sustainable citizen-centric urban solutions that integrate advanced technology with societal needs [47,67]. This can reduce the trading cost, as there is no need to use a central broker in the distributed consensus of blockchain [26,33,47,66,67].

The intersection of IoT, blockchain, and Industry 5.0 goes beyond technological advancement; it represents a shift toward decentralized, transparent, and human-inclusive systems. By addressing critical issues such as interoperability, security, and trust, blockchain and IoT integration not only supports the industrial goals of automation and efficiency, it also ensures that these systems are aligned with the evolving ethical and human-centric priorities of Industry 5.0.

4.2. AI in Blockchain

Artificial Intelligence (AI) can be applied to various aspects of blockchain technology to enhance its functionality and utility AI algorithms can analyze smart contracts deployed on a blockchain to identify vulnerabilities and potential problems. They can monitor blockchain transactions in real-time to detect fraudulent activities, such as double-spending, phishing attacks, or suspicious transaction patterns. AI can be used to develop advanced cryptographic techniques that enhance privacy on blockchain networks. AI algorithms can validate data stored on the blockchain by cross-referencing it with external sources to ensure the accuracy and integrity of data entries.

AI can analyze transaction patterns and user behavior on the blockchain to detect unusual or fraudulent activities. Its algorithms can provide insights and recommendations for decision-making within Decentralized Autonomous Organizations (DAOs). It can optimize consensus mechanisms and network protocols to address scalability challenges in blockchain networks. Natural Language Processing (NLP) algorithms powered by AI can analyze text data on the blockchain, such as transaction memos, which is useful for sentiment analysis. AI can optimize resource allocation and also ensure efficient use of computing power and energy. Predictive AI models can analyze market data and predict the price movements of cryptocurrencies and tokens. In general, AI can enhance various aspects of blockchain technology, including smart contract analysis, transaction monitoring, advanced cryptographic techniques, data validation, fraud detection, decision-making in DAOs, resource optimization, and price prediction. The convergence of AI and blockchain drives significant technology advancements and various industries.

1. Convergence of AI and blockchain:
   The convergence of AI and blockchain [59] represents a powerful synergy that has the potential to drive significant advances in technology and various industries.
   - AI can improve several aspects of blockchain technology, such as security, supply chain, data storage, authenticity validation, healthcare, and financial services.
   - AI protocols can be integrated into blockchain in several formats, such as the use of smart contracts on blockchain platforms to automate and execute AI-related tasks and to manage AI training, data transactions, and payments. Table 3 presents protocols and platforms for smart contracts in AI applications.

Table 3. Protocols and platforms for smart contracts in AI applications.

Protocols and Platforms	Specific Use Cases for Smart Contracts in AI Applications
Ethereum (ERC-20 and ERC-721)	Use ERC-20 tokens to represent access to AI services or datasets. Create decentralized AI data marketplaces where data providers tokenize their datasets as ERC-721 NFT
Binance Smart Chain (BEP-20)	Allow token holders to vote on AI model updates, data access policies, and funding decisions. Issue BEP-20 tokens to represent AI services
Chainlink	Allow token holders to vote on AI model updates, data access policies, and funding decisions. Issue BEP-20 tokens to represent AI services
Avalanche (AVAX)	Integrate Chainlink's decentralized oracles to fetch real-world data for AI applications.
Harmony (ONE)	Avalanche (AVAX) Utilizing AVAX tokens for transactions. Smart contracts ensure secure data exchange and compensation
Polygon (formerly Matic)	Create decentralized governance structures on Polygon for AI decision-making

Blockchain-based AI data marketplaces are designed to facilitate secure and transparent data sharing for AI development and research. Table 4 presents some commonly used protocols and platforms for creating blockchain-based AI data marketplaces.

Table 4. Blockchain-based AI data marketplaces for AI applications.

Blockchain-Based AI data Market Places	Specifications
Ocean Protocol	It allows data providers to publish datasets as "data assets" and provides tools for data access control and pricing
Bluzelle	It allows data owners to share encrypted data securely.
IoTeX	It provides a scalable and secure solution for storing and accessing data in blockchain-based AI applications.
IOTA	It is designed for the Internet of Things (IoT) but can be adapted for AI data marketplaces.
Streamr	It provides a scalable and seamless environment for data transactions.
Polygon (formerly Matic)	It is built on Ethereum, and Streamr's DATAcoin (DATA) is used for transactions.

4.3. Blockchain Tokenization for IoT-Enabled Smart Assets

The application of blockchain technology to create unique digital representations or tokens for Internet of Things (IoT) devices is a hot research topic today. By tokenizing IoT assets, the aim is to enhance their management, security, and value proposition. This approach takes advantage of the decentralized and immutable nature of blockchain to establish secure ownership, track asset lifecycle, and facilitate efficient data exchange between IoT devices and other systems. In general, the tokenization of IoT assets improves their management, security, and value proposition by leveraging the decentralized and immutable nature of blockchain.

4.4. Non-Fungible Tokens (NFTs)

Unlike their fungible counterparts, non-fungible tokens (NFTs) possess distinct indivisible characteristics. Each NFT carries unique properties or metadata differentiating it from others. Although commonly associated with tangible assets such as art, real estate, or collectibles, NFTs can theoretically represent currency. However, the inherent divisibility and interchangeability required for monetary transactions pose challenges for NFT-based currencies. To function as a currency, NFTs require improved specialized mechanisms for fractional ownership and divisible units, an area that is currently underexplored. In general, NFTs have unique properties and can represent tangible and intangible assets. Although challenges remain, they offer potential security and authentication in IoT applications.

4.5. NFTs in Security and Authentication

The distinctive traits of NFTs, including unique digital identities and immutable records, position them as potential game-changers in security and authentication. Their application in domains such as supply chain management, access control, and decentralized identity verification is evident. Nevertheless, while the potential of NFTs for enhancing IoT security is recognized, a significant research gap persists.

5. Requirements for Integrating Blockchain into IoT

Integration of blockchain technology into the IoT could solve many security problems. Securing data transfer in IoT networks is the primary challenge, and is an area where blockchain has an advantage over current solutions [33,39]. As discussed in the previous section, blockchain provides an ultimate solution to problems of trust and many other security issues [39,67,69]. Even though it offers many solutions, it is still a new technology, and integrating Blockchain into IoT systems is challenging. Thus, several requirements must be fulfilled to realize high distribution performance and scalable IoT networks [51,53,70,71]. In general, to successfully integrate blockchains into the IoT, it is necessary to address privacy, access control, security, efficiency, data integrity, authenticity, adaptability, decentralized data storage, low latency, resilience, and ease of deployment. Table 5 compares IoT and blockchain technologies based on these characteristics.

Table 5. Comparative analysis of IoT and blockchain.

Items	IoT	Blockchain
Privacy	Lack of Privacy	Safeguards the privacy of the involved nodes
Scalability	Numerous devices	Scales poorly with Large network
Bandwidth	Limited resources and bandwidth	High consumption
Resources	Resources restricted	Consumes lots of resources
Latency	Low Latency	Block mining it consumes lots of time
Security	Security is an issue	It is more secure

- Privacy: One of the basic requirements for this integration. The blockchain should guarantee the privacy of the user's data when integration is performed [33,51]. This makes a huge difference in the network, as a decentralized environment guarantees that users' information and data are not being tracked or stored [39,51,69].
- Access Control: This should provide access policies and regulations regulating who can view and share users' data both within and outside the network [51,53,70]. Any user who wants to access information should go through these rules and regulations.
- Security: The leading reason for integrating blockchain into IoT is to enhance the security of the IoT network through new design architectures. Data confidentiality and security must be addressed when integrating an IoT system [39,51,69]. The decentralized nature of blockchains promises a massive change in IoT development.
- Efficiency: The integration system should offer minimal performance even though the nodes are present in various subsystems within devices [51,53,70]. This minimal performance certainly increases the efficiency of the device in the system.
- The security and protection of data are significant challenges that IoT devices frequently encounter [39]. To maintain data consistency, accuracy, and protection in a decentralized setting, it is vital to have dependable data when incorporating blockchain into the system [39,51,53]. As previously mentioned, blockchain technology meets this requirement.
- Authenticity: Data transfer in the network is one vulnerability that each user can be exposed to. Data transactions must go through authentication and validation in the system and decentralized computing environment [39,51,69,71].
- Adaptability: The design of a network should possess the flexibility to adjust according to environmental changes, aligning with the various consumer groups and their requirements [39,51,53] Achieving this can introduce several challenges in future applications, particularly in sustaining acceptable levels of system throughput, security, and latency.
- Decentralized Data: The integration architecture should extend the storage size of IoT devices based on the storage capabilities of blockchain technology, which is more accessible in handles [51,53,69].
- Low Latency: The integration of the system should consider delays during computation processes, the same as data transmission from one node to another [39,53]. To keep low latency, it is essential to identify what computation tasks are involved, such as from architecture. It should be decided whether they should be performed at the end of devices, in the dew server, or another layer [39,51,71].

Several requirements should be met, such as resilience; testing should ensure that the failure of a single node does not compromise the entire system [69]. Another requirement is deployment, mandating that all nodes must seamlessly join the network, apart from standard configurations. Blockchain technology offers superior solutions to the challenges faced by IoT systems [39,67,69,70]. Furthermore, smart contracts are key to integrating blockchain within the IoT. Defined as self-enforcing code, smart contracts enable the system to implement agreements triggered by specific events, while blockchain processes these automatically [39,51,69,71]. These contracts are activated when predetermined conditions logged as transactions in the blocks are fulfilled. Operating in a digital realm, these allow for the creation of algorithms that execute specific tasks autonomously while adhering to agreed-upon terms without human intervention. Smart contracts possess unique addresses, are embedded in the blockchain [39,51,67,70], and are executed on each node independently across the network. The blockchain network functions as one computer, with each node operating as a virtual machine [33,39].

The consensus protocol ensures that nodes execute efficiently. Although many blockchains use smart contracts, Ethereum was the first to adopt them. Ethereum is a publicly distributed operating system and blockchain-based platform, and its token is the second-largest cryptocurrency after Bitcoin [49,51]. Launched in 2015, Ethereum was designed as a programmable blockchain to facilitate the creation of decentralized applications [39,49,51,69]. Applications built on Ethereum are reliable and incorporate the advantages of blockchain and cryptocurrency [51]. Smart contracts are first uploaded to Ethereum, where they execute automatically. Execution requires a 'gas fee', which the node executing the smart contract must pay. Smart contracts are linked to both code and data storage [33,39,51] written in Solidity, a high-level language for writing Ethereum operations and contracts. Initially proposed to harmonize IoT with blockchain [33,39,51,67,69,70], smart contracts result in self-sufficient systems that not only fund consumed resources but also manage IoT assets. They also log all IoT interactions, delivering trustworthy and secure processes that effectively support IoT applications [49,51,67].

6. Implementation/Integration of Blockchain and IoT

Blockchain technology is a tool that allows each transaction to be verified in a secure, distributed, and transparent ledger [62,69]. Compared to cloud computing blockchain, it uses the P2P setting, which is decentralized, keeps and processes the information, and does not use the usual client-server architecture. As we know, blockchain has protocols to construct knowledge as chain blocks [39,62,67,69]. In the P2P architecture of blockchain, each peer in the network depends on four functionalities: wallet, routing, services, and storage [61,72]. The blockchain technology for each transaction uses nodes, which makes the blockchain technology secure. In Table 6 below, we illustrate the analysis of the most common type of blockchain, namely, Bitcoin. In this case, routing is an integral part of the Bitcoin network; each node in the P2P network must have a function for each transaction and block propagation [62,69,70,73].

Table 6. Functionalities of nodes in the Bitcoin network.

Node	Storage	Wallet	Routing	Mining
Bitcoin Core	Yes	Yes	Yes	Yes
Solo Minor	Yes	No	Yes	Yes
Full Node	Yes	No	Yes	No
Light Wallet	No	Yes	Yes	No

For the Bitcoin example, in some of the nodes in Table 5, the storage function is needed to keep a copy of the chain, whereas the entire chain is stored in the case of full nodes. To perform the transaction for a different reason, it is necessary to use the wallet service, which plays an important role in providing security in the transaction [61,72]. Lastly, in mining, the main characteristic is the building of new blocks utilizing proof of work (PoW); also known as mining, PoW is performed by certain nodes, which are called miners. Miners receive rewards for each newly generated Bitcoin, and charge fees for each transaction [39,62,69]. The main objective of mining is to strengthen trust in the blockchain network. When a miner finishes a job, the new block is granted the right to be published to the network. The role of peers in the network is to verify the validity of the block before it is added to the chain. The blockchain can be divided into different branches. This happens when blocks in the network are generated simultaneously [39,51,61,62,67,69,72]. The objective of applying blockchain technology in the IoT is illustrated in Figure 13.

The concurrency and intensity of block generation create a unique distributed technique. Blockchains are secure because a malicious node intending to corrupt or modify a block in the blockchain would run out of resources due to the very high complexity of block generation. Thus, the trusted branch of blocks would invalidate any block generated by the intruder. This complicates hacking attempts, as adding a modified or corrupted block to the chain is necessary to solve the PoW before the rest of the miners at the network [39,49,51,67,69].

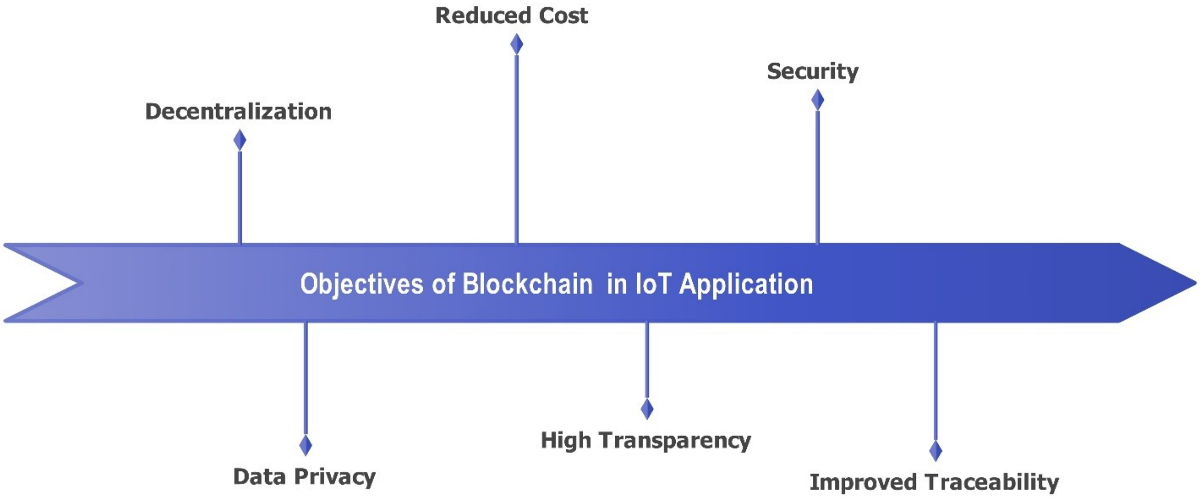

Figure 13. Objective of blockchain in the Internet of Things.

6.1. Blockchain Integration with the IoT

The IoT is revolutionizing the world by creating more interconnected devices that automate and optimize manual procedures, generating increasing amounts of data that improve people's lives [62,69]. Previously, cloud computing was the only option that provided IoT devices with essential services, allowing them to process and analyze information and convert it into real-time services. With the growth of IoT devices, challenges such as the open data paradigm, centralized architecture, and lack of confidence have emerged [70,73,74].

Blockchain improves IoT technology by providing shared resources in a reliable and traceable manner. Data sources can be securely specified and kept unchanged, as many IoT devices share information securely [39,62,69]. This knowledge or information can help people build smart applications that improve management and lifestyles. Figure 14 illustrates the model for integrating blockchain into the IoT. Overall, blockchain technology is a tool that allows each transaction to be verified in a secure, distributed, and transparent ledger. Compared to cloud computing, blockchain uses a P2P setting which is decentralized, allowing it to maintain and process information without the usual client-server architecture. Blockchain protocols construct knowledge as chains of blocks. In the P2P architecture of the blockchain, each peer in the network relies on four functionalities: wallet, routing services, storage, and mining.

Additionally, Blockchain actively enhances IoT services through the following methods:

- Security— How IoT devices can achieve full benefits by storing information and securing communications in the way they do is by using the transaction property in introducing blockchain technology [62,69]. Another critical method in the blockchain is used to validate the message exchange through different devices. The way this is done is by using smart contracts. Smart contracts play an essential role in blockchain technology and the optimization of the security of protocols for IoT applications [39,62,67,69]. Overall, IoT devices achieve full benefits by storing information and secure communications using transaction properties in the blockchain. Validating message exchanges through smart contracts and security protocols optimized for IoT applications plays crucial roles as well.
- Traceability and Reliability—Blockchain can improve IoT applications and devices by distributing information and keeping it unchanged [62]. Moreover, blockchain can help to verify data authenticity and ensure that the presented data remains untouched while in transit. Data are traced for identification and protection. Blockchain technology enables sensor data accountability and traceability [49,51,67,70]. Reliability is one of the key aspects blockchain brings to IoT. Overall, blockchain improves IoT applications by distributing information and keeping it unchanged. It verifies data authenticity, ensuring that the data remains untouched during transit. Sensor data accountability and traceability are enabled through blockchain as well.
- Decentralization and Scalability—The main points that lead to failure phenomena and bottlenecks typically occur in the client-server architecture. That is why cloud computing will be eliminated by the shift to P2P, decentralization, and servers utilizing blockchain technology [62,69]. Additionally, controlling information generated by IoT applications storage and processing by powerful intermediaries is prevented. Each shift performed by the blockchain improves fault tolerance by default and permits idealistic IoT scalability [49,51,62,69]. Overall, blockchain-based P2P decentralized and server-less architectures prevent the failures and bottlenecks common in client-server models, resulting in improved fault tolerance and allowing for ideal IoT scalability.
- Identity—Each device on a blockchain is uniquely identified. Every additional frame sent to the network and used by it is immutable; this includes the sender's address, making it hard to spoof blockchain devices [39,67]. This advantage prevents spoofing attacks that may be present in IoT and other wireless devices [39,51,67].
- Service Markets—Transactions using blockchain technology are anonymous, and because transactions take place between peers, they are also decentralized. This eliminates the need for a central authority, which can speed up the creation and sharing of newly created business applications. In addition, it is not convenient to deploy microservices to allow the dispatching of small payments safely [61,62,69]. Overall, blockchain's anonymous transactions between peers eliminate authorities, speeding up business application creation and microservices deployment.
- Autonomy—Internet of Things applications and devices can also benefit from blockchain by its elimination of dependency on servers, helping to spread decoupled device-agnostic applications [49,51,69].

Integrating Blockchain technology in IoT systems involves determining where interactions should take place, choosing among internal IoT, hybrid design, or exclusive blockchain use [70,73]; in hybrid approaches, a new intermediary layer between cloud computing and IoT devices is crucial. Below, we provide an analysis of these three options:

1. Inside IoT—This method offers rapid response and high security by allowing offline interactions, enabling IoT devices to communicate directly with each other, including routing and discovery operations. Not all IoT data are stored on the blockchain, and devices can communicate independently of it. This method is highly suited for scenarios where reliable IoT data exchange with low latency is vital [39,62,69]. In essence, this approach permits direct communication between IoT devices with low latency, omitting blockchain for data storage.

2. Hybrid—In hybrid layouts, some interactions and data persist on the blockchain, while others are shared directly among IoT devices. A key challenge is determining which transactions should utilize the blockchain to influence runtime decisions [61,72]. A prime example of this is the integration of blockchains with IoT utilizing blockchain's advantages alongside real-time IoT interaction. This method combines fog and cloud computing to address the constraints of both blockchain and IoT [39,62,67,69]. Fog computing involves less powerful computational devices such as gateways, and supports initiatives similar to mining using IoT devices. Figure 15 illustrates the intricacies of IoT infrastructure and its operations. The cloud's capabilities facilitate communication, while end-users can also engage with the cloud. In summary, some data and interactions are processed by the blockchain, with the remainder shared through real-time IoT communications. Fog and cloud computing enhance the functionality of both blockchain and IoT.
3. Blockchain–IoT—By registering all transactions on the blockchain, a permanent record of interactions is created [67]. This approach supports selecting a traceable exchange, as information can be retrieved from the blockchain, thereby enhancing the autonomy and presence of IoT [51,62,67,69]. IoT benefits from this strategy include fulfillment of the required services. However, documenting every interaction on the blockchain necessitates enhanced bandwidth and data management, presenting a significant challenge. In this context, the IoT data related to these transactions are stored directly on the blockchain [39,67,69]. Generally, all interactions are conducted via blockchain, providing a non-alterable record. While this method guarantees traceability and independence, it demands greater bandwidth and data processing capabilities.
4. Comparison of IoT–Blockchain Integration Protocols—In IoT–blockchain integration, several commonly explored protocols are used to address the unique demands of IoT networks: Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), and HTTPS. MQTT is designed for constrained networks and is advantageous in low-bandwidth environments due to its lightweight nature and efficiency in handling large volumes of IoT data. CoAP also offers a resource-efficient approach designed for simple devices in IoT ecosystems, with lower overhead compared to HTTP. Although HTTPS provides robust security through TLS, its higher computational load can limit its effectiveness in resource-constrained IoT settings. Each protocol presents distinct tradeoffs in terms of security, scalability, and resource efficiency, making protocol selection a critical consideration in IoT–blockchain integration.

6.2. Challenges in Blockchain–IoT Integration

Integrating blockchain into IoT is challenging due to the differing sizes of blockchain data and IoT user data. The size of blockchain data, such as Ethereum and Bitcoin, ranges from 250 GB to 1 TB, which is large compared to IoT devices [67,73]. This discrepancy poses challenges when seeking to fully implement blockchain in IoT devices. One solution is to use cloud computing to store block data, with only hash chains stored in IoT devices. The use of applications in IoT technology represents a motivation to use blockchains for secure data transfer in IoT networks. This advantage can solve many security-related problems [34,67,75] In addition, transactions on a blockchain network are signed digitally. It is necessary to equip IoT devices to operate and use a blockchain [51,67,73]. Before more deeply analyzing the integration of blockchain into IoT, it is important to review several challenges and concerns that arise from this integration. Figure 16, these challenges include:

- Size of Blockchain Data: There is a significant difference in the fixed and operational size of user data between what blockchains typically offer and the Internet of Things [34,67,75]. The size of blockchain examples varies based on which chain is being used; for example, Ethereum and Bitcoin have sizes of 250 GB or 1 TB at present now, which is large compared to the typical data size used by IoT devices [38,67,69,73]. This vast difference in size can present a challenge, as IoT devices may not have the space or storage capacity to process blockchain data [38]. Size issues can become an obstacle to fully deploying blockchains in IoT devices [34,67,69,75]. However, there are many ideas on how this challenge can be solved. One way involves using cloud computing [38,67] to solve the problem via additional storage. In this approach, block data are stored in the cloud, where only some light data such as the hash chain held by IoT devices [39,67,69,70]. At present, this is the best solution regarding the different sizes of blockchain and IoT data, even though it can create a conflict when cloud computing is centrally controlled and blockchains are decentralized [34,51,67] (Figure 17).

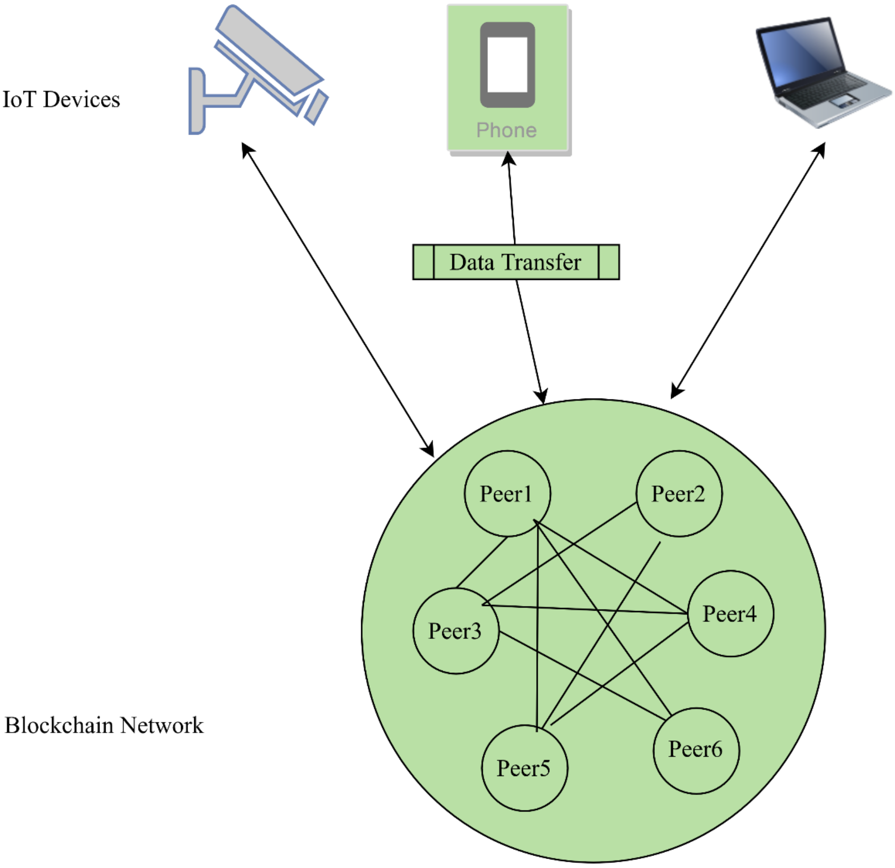

Figure 14. Blockchain–IoT integration model.

- Security: IoT applications face significant security challenges, including issues related to device performance and the high heterogeneity of devices. While blockchain is considered a potential solution, its integration with IoT raises concerns about the reliability of IoT-generated data. Blockchain ensures data integrity unless the data are corrupted at the source from the IoT devices [38,69]. However, the increasing frequency of attacks on IoT networks has led to severe consequences, highlighting the need for technology that enhances device security. Many experts [67,69,75] view blockchain as a promising solution to address security in IoT. However, the integration of blockchain with IoT also brings its own set of challenges [67,69,73], one of which is ensuring the reliability of the initial IoT-generated data. While blockchain can guarantee the immutability of data within the chain and track any modifications, if data becomes corrupted, the blockchain makes this permanent. Thus, while IoT data can be vulnerable to corruption [34,39,51,69], and blockchains can secure the integrity of data processed through them, this relies on the data not being maliciously altered by the IoT devices themselves [34,67,70]. Therefore, data corruption represents a critical issue, with potential causes including device malfunctions, hacking, and the presence of fraudulent IoT devices [34,67,69,75] (Figure 17).

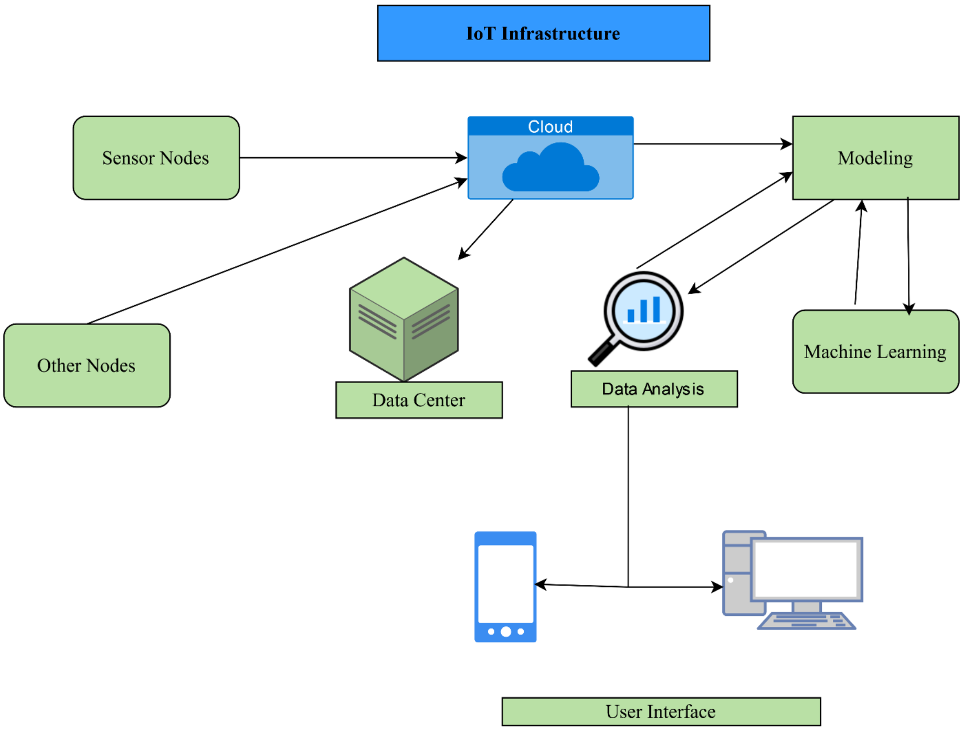

Figure 15. Internet of Things infrastructure.

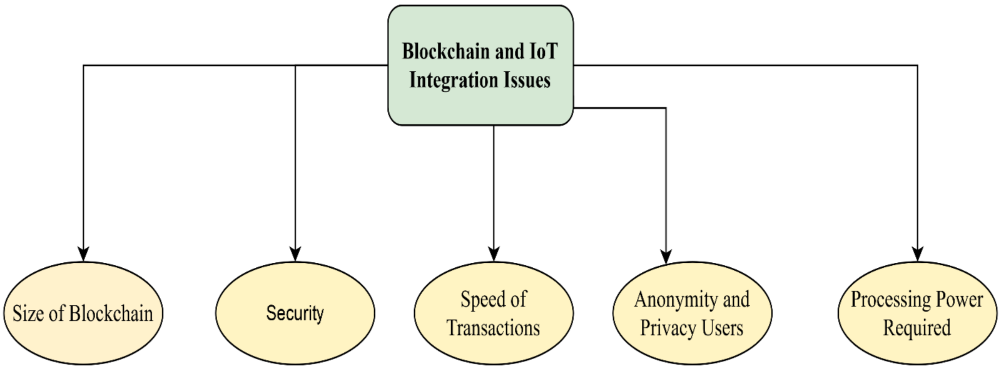
Blockchain and IoT Integration Issues
Size of Blockchain
Security
Speed of Transactions
Anonymity and Privacy Users
Processing Power Required

Figure 16. Integration issues of IoT and blockchain.

- Anonymity and Privacy: Many IoT applications manage sensitive information; when a device is linked to an individual, such as in e-health applications, safeguarding data privacy and anonymity becomes a critical issue [39,67,69]. Blockchain technology presents a potential solution, with examples such as Bitcoin ensuring user anonymity [34,69,70]. However, securing data privacy in IoT is more challenging, as it involves securing data at the collection, communication, and application layers. Protecting devices where data is stored and preventing unauthorized access necessitates the integration of cryptographic security software into these devices [34,69]. Leveraging cryptographic hardware in the cloud can reduce the complexity of security software and speed up cryptographic processes [38,67,69,75]. Additionally, various international regulations, such as the EU's data protection laws [34,51,69], govern the privacy of data. Therefore, adopting blockchain technology must align with these regulations and adhere to legal standards [34,69,75]. Ensuring data privacy and building trust are critical challenges for IoT. Blockchain can address identity management issues in IoT by maintaining data integrity while managing large volumes of data and providing efficient and controlled access. Compliance with global data protection laws is essential for the effective implementation of blockchain technology [34,69,75] (Figure 17).

- Speed of Transactions: The transaction rate is one of the most important differences between different blockchains, and is one of the biggest problems when integrating blockchain technology with IoT [34,67]. Thus far, the rate of blockchain systems such as Ethereum and Bitcoin is not more than 4 to 5 transactions per second, and the systems that are meant to be integrated with IoT are slower. IoT systems generate a large amount of data in real-time which is too fast to be synchronized with the speed of blockchains [39,67,69,73,75]. Blockchain was not intended for holding and processing the amount of data that IoT devices can produce; as a result, there is a gap in terms of transaction speed. Overall, the slow transaction rate of blockchains compared to the data generation rate of IoT devices poses challenges for real-time IoT integration.

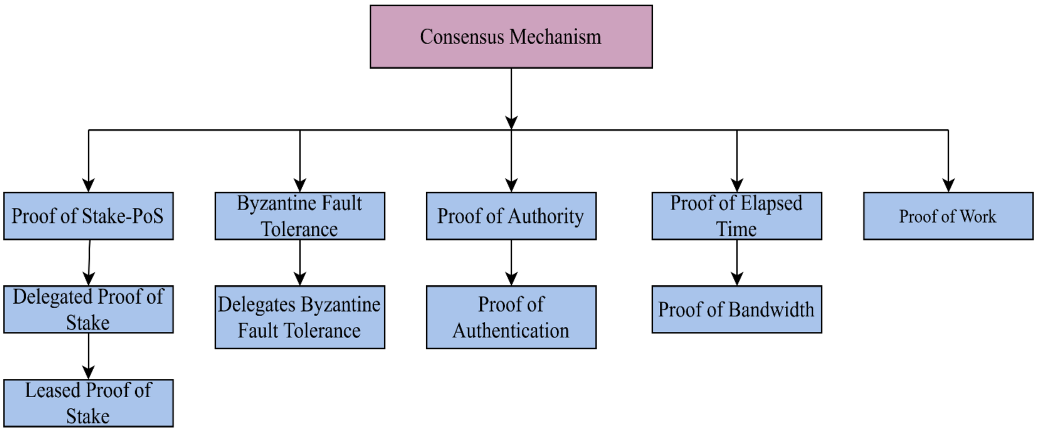

Figure 17. Taxonomy of consensus mechanisms.

- Legal Concerns: The unregulated nature of blockchain technology is a fundamental element of its design, and has contributed to Bitcoin's success within the financial system [34,70,75]. However, this lack of regulation, particularly around virtual currencies, has raised numerous legal questions [39,67,69,75]. The incorporation of control mechanisms such as permissioned, private, and consortium blockchains addresses some of these concerns. Similarly, the Internet of Things (IoT) sector is influenced by national laws and regulations regarding data privacy and usage [69,70,73]. Many existing laws are becoming outdated due to rapid technological developments such as those involving blockchain technology. Creating new regulations could ensure the security of devices and enhance the reliability and safety of IoT networks [38,69,75]. Despite regulatory changes, challenges persist in managing information privacy and security [69,70]. Certain IoT devices use a global unique blockchain for machines, although it remains unclear whether these networks can be controlled by manufacturers or open users [34,39,51,67,69,75]. The continuous evolution of laws and regulations will influence the future of both blockchain and IoT, potentially compromising blockchain's decentralized and free nature by introducing centralized government or regional control [69]. In summary, the unregulated status of blockchain creates legal challenges, particularly around virtual currencies, and both blockchain and IoT are affected by data privacy laws that require updates to keep pace with technological advances.
- Latency and Power Consumption: Latency is a critical consideration in IoT applications where real-time processing is essential, while transaction validation delays inherent to many blockchain systems can hinder the timely flow of information. Additionally, the energy demands of certain blockchain processes, particularly in consensus mechanisms such as PoW, can quickly drain battery-powered IoT devices. For resource-constrained IoT environments, lightweight consensus algorithms and optimized block sizes are needed to manage power consumption while maintaining

security and efficiency. These constraints underscore the need for tailored blockchain solutions in IoT.

7. Blockchain Security

Although blockchain is considered secure, recent studies have shown vulnerabilities to various cyberattacks affecting both its availability and integrity. Exploiting these vulnerabilities can compromise data recorded in the ledger, negatively impacting the blockchain state [26,33,39,45,56]. In addition, many programs are exposed to vulnerabilities that attackers can exploit. Attackers could gain unauthorized access to the blockchain and harm it if there is some way to perform a malicious operation [33,56,59]. Exploiting vulnerabilities in the blockchain can result in data becoming compromised, and compromised data recorded in the ledger could negatively impact the state of the blockchain [26,39,45,56,60,75]. Blockchain uses a 160-bit address space, which is hashed by a public key generated by the Elliptic Curve Digital Signature Algorithm (ECDSA) [33,39,58]. A large number of particular addresses have been developed and allocated for assignment to IoT devices, each of which is unique [34,45,58,59].

Because blockchain provides a unique address, transactions in the blockchain cannot be altered and can be traced back to guarantee data reliability [26,33,58]. Another advantage of blockchains that use smart contracts is that they provide decentralized authentication logic that is hard-coded and simple, making it easier to authorize IoT devices [33,45,58,59,75]. Using smart contracts, it is possible to set different rules to update IoT software, establish new key pairs, and change ownership [45,58]. The following subsections provide an overview of blockchain security, blockchain-based IoT cyberattacks, and countermeasures.

7.1. Blockchain-Based IoT Cyberattacks

Cyberattacks on blockchain-based IoT systems can originate from inside or outside the network. External attacks come from attackers unfamiliar with cryptographic keys, while internal attacks involve trusted insiders. An outside-network attack is an external attack that occurs when an attacker does not know much about the cryptographic network keys and starts to attack from outside the network [45]. In contrast to an external attack, in an internal attack, the attacker has control and is trusted [4,34]. This section discusses common cyberattacks, including Sybil, eclipse, and DDOS attacks.

1. Sybil Attack: This attack involves a malicious party controlling a blockchain network by owning multiple malicious nodes [45,56,58,73]. Sybil attacks manipulate transactions or flood the network with bad transactions. PoW makes Sybil attacks expensive to execute, requiring significant computational resources [45,73,76,77]. Certain blockchain networks use consensus protocols alongside PoW to prevent Sybil attacks. Furthermore, to launch this attack an attacker must use many computational resources to produce a block. PoW makes Sybil's attacks expensive to launch. For instance, the attacker may require many native cryptocurrency coins to add a new block to the blockchain [56,73]. When an attacker succeeds in this kind of attack, they can compromise the entire network by manipulating a large number of virtual nodes in the network; thus, several blockchains use consensus protocols in conjunction with PoW to avoid Sybil attacks [56,58,73,77]. In this case, PoW is conducted after every 100 blocks [34,42,45,73]. Several solutions have been offered to prevent Sybil attacks. In [45], an IoT trust model was proposed for each user permission blockchain with smart contracts to evaluate the trustworthiness of IoT device identities. Sybil attacks may occur due to the confusion some nodes can experience after a hard fork, which often happens within insecure cryptocurrency-based protocols. One cryptocurrency that is still vulnerable to Sybil attacks is Ethereum [42,56,73,76], as it has weak restrictions on the node generation process [34,56,77].
2. Eclipse Attack: In an eclipse attack, an attacker isolates victim nodes from the normal blockchain network by stealing routing tables and adding fake nodes as neighbors [34,42,56,76]. Eclipse attacks can lead to issues such as route fraud, storage

squeeze, and denial of service. This attack is closely associated with Sybil attacks, often requiring multiple malicious nodes. Research on eclipse attacks has shown their severe impact on network topology and resource-sharing efficiency. Furthermore, when an eclipse attack targets a victim node, most of its external route paths are controlled by the attacker nodes [73,76]. When nodes are attacked, they can take actions such as route fraud, storage squeeze, denial of service, and more. Thus, eclipse attacks represent one of the most severe threats to blockchain networks [45,73,76]. Eclipse attacks usually require more nodes than Sybil attacks [34,42,56,77]. One study reviewed for this article introduced an eclipse attack on the Bitcoin P2P networks. The eclipse attack destroys network topology, which reduces the number of nodes and the efficiency of resource sharing [34,45,73,77]. A consequence is that the attacker hijacks blockchain network requests and falsifies the received replies, meaning that normal sharing and downloading cannot be performed [34] (Figure 18).

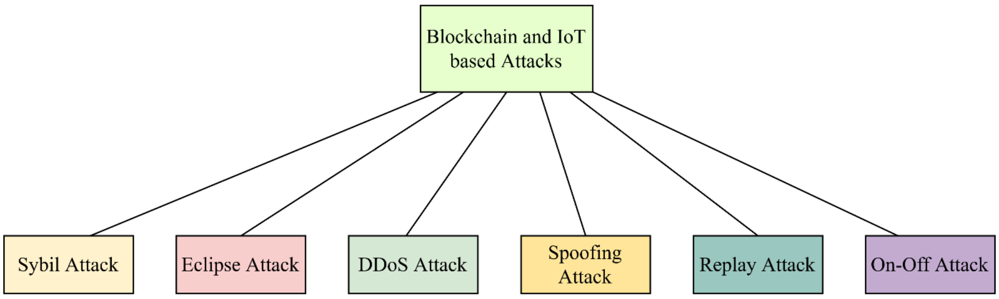

Figure 18. Blockchain and IoT-based cyberattacks.

3. DDoS Attack: Distributed denial of service (DDoS) attacks are a major threat to blockchain networks connected to IoT devices [34,45,76,77]. In a DDoS attack, the attacker uses a client-server model to combine multiple computers, amplifying the power of denial-of-service attacks. This multiplication of resources targets multiple nodes simultaneously, using the blockchain as a DDoS attack engine [34,42,56]. This happens because many (millions) of online nodes concurrently hold many resources in storage and bandwidth, and a blockchain node needs to keep a copy of the whole network [34,56,76,77]. DDoS attacks can be divided into active and passive attacks. Active DDoS attacks work in the way described above.
   The attacker actively sends a large amount of false information to the network node; subsequent visits to this information are then forwarded to the victim. Passive DDoS attacks are based on a push mechanism in the blockchain network protocol [34,42,73]. This results in a lot of information being generated within a short period, which is not easy for the network to record and analyze. This allows the attacker to avoid IP checks by using fake source addresses, making it difficult to track and locate the attack sources [34,42,45,76,77]. Blockchain-based passive DDoS attacks wait for queries from other nodes and then modify the blockchain client/server software to return an incorrect response to achieve an attack effect. The goal of the attack is to deploy multiple attack nodes, which include target hosts, in one response message [34,56,77]. This attack deploys the pull mechanism in the blockchain network protocol.
   DDoS attacks can be facilitated by Sybil or eclipse attacks [34,45,56,68]. The goal of Sybil attack is for each physical node to generate many different identities on the blockchain network. On the other hand, DDoS attacks on a single node send many false messages to the network or provide incorrect responses [34]. Another way to launch DDoS attacks is by using only one computer to repeatedly exploit an intelligent contract, thereby congesting the network with megabytes of bytecode [42,73,76,77].
4. Spoofing Attack: Another meaningful attack type consists of spoofing attacks. A spoofing attack attempts to assume the identity of a legitimate user, possibly by using false or virtual identities created during a Sybil attack and using its privileges to exploit

the network [45,58,73,77]. The identity used in a spoofing attack can pretend to be a legitimate user of an IoT device, such as by using a legitimate user's IP address or MAC address [42,45,76,77]. In this way, the attacker can gain unauthorized access to the IoT network and open doors to exploit other attacks that can seriously damage the network [45]. Table 6 shows the types of attacks and what layer they target.

5. Replay Attack: In a replay attack, a valid transmission is maliciously repeated [34,42,45]. A blockchain replay attack occurs when the blockchain is a hard fork and a transaction from one chain is replayed on another [34,42,77]. Because there are two chains and both transactions are valid, their addresses are the same, as is the algorithm used to generate the private key, meaning that the transaction information is the same. This results in a transaction on one of the chains that is likely to also be perfectly legal on the other [34,45,56,76,77]. A replay attack occurs because verification of the message does not certify the correctness of the message's sending time; any messages can be selectively captured and replayed later without alteration by the attacker [45,73,76]. Message replay attacks are often combined with message removal attacks [45].
6. On–Off Attack: In this attack, a malicious node behaves both well and poorly. This behavior attacks before the trust system becomes aware of it [42,45,58,76]. On-off attacks are known as selective attacks, as malicious nodes can attack multiservice IoT architectures by acting according to the type of service they provide to other nodes in the network [34,42,45,56,77]. On–off attackers behave differently with different neighbors to obtain contradictory trust opinions for the same node. This type of attack is hard to detect because it uses traditional trust management schemes. Classifying a node's behaviors requires prior trust knowledge and time, and not all malicious devices necessarily misbehave [45,76,77].

7.2. Countermeasures

To protect against cyberattacks against blockchain-based IoT systems, several countermeasures can be implemented. The following subsection discusses countermeasures against physical attacks, network attacks, and software attacks.

1. Countermeasures Against Physical Attacks: When it comes to physical attacks, a mutual authentication protocol has been proposed based on PUF (Physically Unclonable Function) for small devices that exploit the inbuilt variability of an integrated circuit [42,44,56,73,76]. Authentication is carried out using the challenge-response mechanism, where the output primarily depends on the device's physical microstructure. In this case, forging the PUF [42] to clone the same structure is impossible, which eliminates attacks such as tampering and malicious code injection [42,56,73]. To address physical attacks, the heterogeneous architecture proposed in [42], which is used on a customizable and trustable device mote, can provide both energy and performance benefits. This architecture uses reconfigurable computing with an IEEE 802.15.3 radio transceiver and hard-core microcontroller unit [34,42,44,73,77] with a Contiki-OS host [42,56]. Another proposed solution is REATO [42,44,56], which deals with different kinds of DoS attacks on IoT devices. It uses a cross-domain and flexible middleware named NetwOrked Smart object (NOS) tailored for REATO [42]. The solution is based on an HTTP connection request to NOS. After validation, the encrypted information is sent back [34,42,56].
2. Countermeasures Against Network Attacks: There are several proposed solutions for defending against network attacks such as replay a Sybil attacks [34,42,56]. One of these solutions involves detecting and isolating the nodes launching Sybil attacks. The trust-aware RPL routing protocol named SecTrust-RPL uses a mechanism based on trust to fulfill this goal [42,56,77]. The framework is attached to ContikiRPL. The purpose is to serve as a trust engine for malicious node detection and making routing decisions [42,44,56,73,76]. Another model is the "signcryption" technique, which is based on Identity-Based Cryptography (IBC) to satisfy the requirements of confidentiality, integrity, and authenticity [42]. This technique combines encryption and

signing and avoids the need to access a trusted third party to fulfill the authentication process [34,42,73]. This method is mainly proposed against replay attacks. Notably, in-network attacks avoid the typical defensive frameworks against network DoS and DDoS attacks related to message flooding [42,56,76,77]. Using a DDoS server from a third party, this approach uses an algorithm for the server consisting of two parts. One part analyzes the incoming traffic to decide on the danger level [42,44,76,77]. This assesses suspicious activity related to DoS or DDoS attacks. The proposed SD-IoT framework uses an algorithm to detect and mitigate DDoS attacks using the cosine similarity of vectors [34,42,44,56]. This works by obtaining a threshold value using the cosine similarity of the vectors of the packet-in-message rate at the SD–IoT boundary [42]. When a DDoS attack is found, a threshold value is used, and the attacker is found out and blocked at the source.

3. Countermeasures Against Software Attacks: Several frameworks have been developed to integrate several different security aspects to protect against Trojan hardware on IoT devices [34,42,44]. The first key aspect is vendor diversity, which enables trusted communication between untrusted nodes. Second, message encryption prevents unauthorized parties from accessing contacts. Lastly, mutual auditing allows authorized nodes to verify the encryption status and content of a message[42,56,76,77]. Another way to prevent hardware Trojans is by using high-level synthesis (HLS). Security improves the hardware produced by HLS, which is an indirect way to prevent the injection of hardware Trojans into the network [34,42,44].

Many Various strategies have been proposed to safeguard against different forms of attacks. One such approach is the greedy heaviest observed subtree rule, abbreviated as GOST, a variant of which has been utilized in Ethernet projects [34,44,56,76]. Initially, it evaluates how Bitcoin's security is affected when throughput is increased. This is achieved by enlarging the block size and the rate at which new blocks are created. While enhancing the blockchain's throughput is possible, it concurrently raises the likelihood of forks in the block tree, thus compromising blockchain security [34,73,77]. This method addresses the security issue by substituting the longest chain principle with that of the heaviest subtree [42,56,73,76,77]. By altering the node architecture, the structural organization of the Bitcoin blockchain, and computing power, dishonest nodes can reach a threshold of 50, thereby securing the whole system [34,42,56,73].

7.3. Blockchain and Privacy Issues

Each user in the blockchain is identified and transacts using their public key, also known as a hash. This guarantees user anonymity even though transactions are shared and everyone can see and analyze them, as users never know each others' identities [26,54,56,64]. For this reason, we say that anonymity is a fundamental property of blockchain technology. This is one of the reasons that Bitcoin and other cryptocurrencies have been so successful, as users can utilize several anonymous addresses for transactions. Many different methods have been taken to fulfill the goal of anonymity [33,34,45,56]. However, researchers have raised questions about the privacy of blockchain technology as well [26,34,58,59,64]. These concerns have mostly been raised because all transactions are publicly logged [34]. With the development of different technologies over the years, privacy concerns have led to privacy being recognized as a fundamental human right by the United Nations in the Declaration of Human Rights as well as in the Charter of Fundamental Rights of the European Union and many other parties and organizations worldwide [33,54,56,64].

Because privacy is one of the main concerns in blockchain technology, privacy itself needs to be determined by the nature and use of each application as appropriate; other requirements can appear, such as cryptocurrency being offered in public such that anybody will be able to contribute by adding transaction in the ledger, which is public. In blockchain, there are no private transactions, as mentioned above [45,51,56,64]. Blockchain can enhance the transparency of the user's communications, such as by providing an audit trail of the underlying data processes. In this case, other data protection requirements may be present [45,51,54,56,58]. In this section, we present some techniques for alleviating privacy issues when using blockchain technology to process personal data. Pseudonymization is available in all blockchain platforms to protect individuals' identities while allowing them to retain the utility of their data [54,56,64]. Pseudonymization can be defined as the processing of personal data such that the data are no longer attributable to a specific individual without the use of additional information. The information is kept separately and is subject to technical and organizational measures to ensure that they cannot attributed to an identifiable individual, which in this case is achieved by replacing users' identifiers with pseudonyms [33,45,51].

Cryptocurrencies such as Bitcoin and Ethereum use pseudonymization techniques; each user's wallet is uniquely associated with a random-looking address. All transactions can be seen by the public, including the amount sent or received and the generated public key or hash; however, there is no inherent way to map the address back to an identified individual [33,56,64]. Bitcoin and Ethereum both use mixing techniques, which allow the shuffling of two or more transactions without revealing the exact relationship between them. This means that transactions can interfere with each other and cannot be linked. Because this technique is old, the blockchain is used to conceal the history, because each transaction stored in the Blockchain is connected to multiple senders and receivers [26,64]. Mixing services can be provided through a centralized mixing service or on a peer-to-peer basis [45,56,58]. This method can be a perfect way to improve privacy, as it aggregates communication between peers in various strategies and output actions. While this technique has been used to expand privacy, it is not complete in blockchain technology, and may not be as present [51,56,59]. The mixing method is also used to confuse attackers, making it hard for them to infer the exact number of real coins spent in transactions [33,45,59,64]. Another technique being presented and operated is the zero coin, also known as zero of knowledge, which is shown to the counterparty to allow users to recognize obvious information [56,58,59]. This helps to verify reliable transactions by preventing user identity detection, although there is evidence that the technique is not immune to attacks [45,56,58,59,64]. In particular, the mixing method may be vulnerable to de-anonymization through statistical detection attacks.

Advanced Cryptography Technologies to Protect Blockchain User Privacy: There have been proposals to solve user privacy issues on public blockchains through smart contracts that automatically generate efficient cryptographic protocols using primitives, i.e., zero-knowledge proofs [45,54,58,64], which have been discussed earlier. Zero-knowledge proofs enable a statement to be verified without any information other than the statement itself [33,51,54,64]. Zero-knowledge proofs are used for many reasons and applied in the concepts of zerocoin and zerocash. Another important security aspect of blockchain is data protection. Data are preserved by confidential transaction technologies [26,45,54,56]. Researchers have [33,45,51,54] have shown to keep the content of transaction example amount being sent or show participant, where it concludes that the content can be verified such that no more coins can be available ones can be spent in a cryptographic means [51,54,64]. Another solution that has been proposed that we did not mention until now is attribute-based encryption (ABE). In this case, secret keys are generated based on the attributes of peers. Applying this method, sensor data in transactions can be encrypted and decrypted using the miners and users using decryption credentials from attribute authorities [54,56,64] (Table 7).

There are other privacy issues in the IoT section, such as the lack of IoT-centric consensus mechanisms [58]. The consensus protocols deployed on different blockchain platforms share a common issue in that consensus finality, while permanently committing new blocks, might result in delayed transactions [50,56,58,78]. Because of this, blockchain seems to be a poor fit for instantaneous IoT systems. Another issue is transaction validation, where some rules may use a different transaction format, signature, and other parameters depending on the blockchain platforms [45,54,78]. An example of this is Bitcoin transaction validation rules, which include checking whether the same transaction has been spent before.

Table 7. Security.

Blockchain	Hyperledge	Ethereum	Bitcoin
Nature	Permissioned	Permissionless	Permissionless
Validation	PBFT	Ethash PoW	PoW
Purpose	Chaincode	Smart Contracts	Crytocurrency
Language	Java, Go	Internet Code	Scripts based in stack

On the other hand, different rules are included in Ethereum, such as checking the balance of the sender account. In addition, other validation rules can be created to meet the heterogeneity of the sense data [50,58]. Table 7 shows how these features work and how they can be used. Data scalability and management issues represent another problem, as a blockchain is a distributed ledger of databases that grows over time because of the massive volume of data collected from a wide range of interconnected IoT devices [50,56,58,78]. Without proper security control, these devices might cause compatibility issues that would result in severe security issues [51,56,58,59]. User experience is another issue; as we know, most applications are built on top of the blockchain, which requires the end user to manage and control their transactions through e-payments instead of using an intermediary such as a bank. The same issue arises concerning the computational power required for the user to mine or commit new blocks [33,50,56,78]. This may cause the blockchain network to be cumbersome when logging transactions due to the complexity of decentralization. These issues are present when blockchains are integrated into IoT.

7.4. IoT Trust Issues and Blockchain-Based Solutions

Security necessities and issues for IoT include the following:

1. Data Privacy—Due to the wide-ranging integration of services and networks, the data stored on devices may be susceptible to attacks by compromising nodes within connected IoT systems [33,51]. Additionally, attackers could access the data without the owner's authorization.
2. Data Integrity—Within a centralized client-server architecture, an attacker might exploit unauthorized network access to alter the original data or information before forwarding it. For example, when Alice sends data to Bob, an intermediary (Watson) could intercept and modify these data before passing them on [45,54,77].
3. Third Parties—Information gathered in a centralized setup is held and managed by an external centralized organization, which might abuse this information or share it with others [45,58].
4. Reliable Data Sources—In the IoT context, identifying the source of data generated by various devices is challenging because the information is stored across the entire network and can be modified by any user [34,56,77].
5. Access Management—One of the primary challenges in IoT networks is access management. Determining which nodes are authorized to access and execute various functions across the entire IoT network can be complex [45].
6. Single Points of Failure—The ongoing expansion of centralized networks for IoT infrastructure can reveal single points of failure. If a central authority stores and verifies all data of the network [58,59,77], then the entire network becomes vulnerable if the main point fails or experiences downtime.
7. Scalability—The Internet of Things interlinks numerous sensors and diverse devices for data exchange and various applications over the internet [64,78]. This poses a challenge to the system's architecture and its ability to grow swiftly and to scale. Figure 19 illustrates the dimensions of scalability, divided into horizontal and vertical scalability, depicting the dimensions of blockchain scalability.

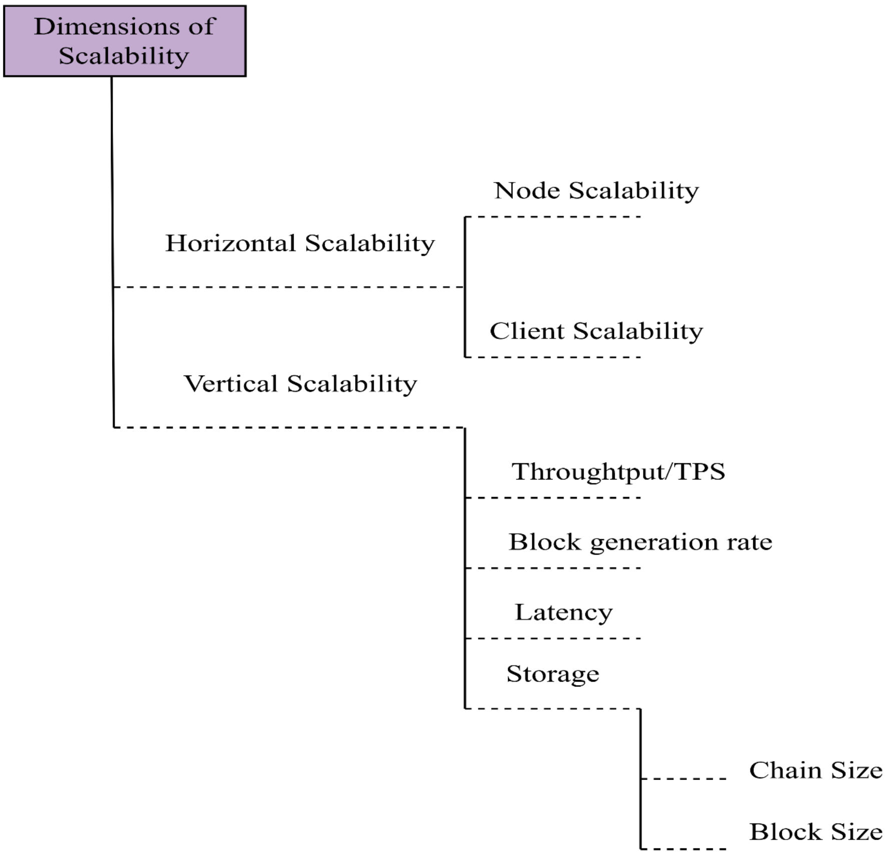

Figure 19. Dimensions of blockchain scalability.

7.5. Blockchain Solutions for IoT

- Data Integrity—Blockchain operates as a peer-to-peer network in which each node maintains a duplicate set of records. When a transaction is initiated, the originating node uses its private key to sign the transaction and then sends it to other nodes for validation. All miner nodes take part in the validation process to find a nonce [34,42,64]. The first node to discover the nonce gains the right to validate the transaction and receives a reward. It then broadcasts the validated transaction to all other nodes in the network. When the transaction is added to the blockchain, it is immutable and cannot be altered, rolled back, or deleted [33,51].
- Data Privacy—A consortium blockchain ensures data privacy within a blockchain network. As depicted in Figure 3, all nodes intended for a specific purpose are grouped to create a private network or sidechain. Each sidechain handles its respective IoT data [34,77]. Nodes belonging to one sidechain do not participate in the validation process of other sidechains. To access data on the consortium blockchain network, a requester node must first register and join the relevant sidechain network, and then submit an access request. Consortium blockchains include access control mechanisms to prevent unauthorized access [34,42,64,77].
- Addressing Space—Blockchain utilizes a 160-bit address, while IPv6 employs a 128-bit address scheme. Consequently, blockchain offers 4.3 billion more addresses than IPv6, offering enhanced addressing capacity compared to the IPv6 addressing scheme [51].
- Trusted Accountability—Each operation record is required to be logged in the blockchain network. This process assigns an identity to every operation, making each one traceable. If any abnormal behavior is identified, it is reported back to the origin for further investigation [8,56].
- Fault Tolerance—Decentralized devices are less likely to fail accidentally, as they rely on many separate components. A blockchain is a point-to-point decentralized network.

Every device has the same record copy in it; thus, a single node failure does not affect the network [45,56]. This makes blockchain resistant to single points of failure.

- Trusted Data Origin—To track data in a blockchain network, a unique ID is assigned to each IoT device [56].
- Removing Third-Party Risk—Blockchain technology empowers devices to execute operations without relying on an intermediary or third party, making them free from third-party risk [51,58,77].
- Access Control: Smart contracts, first proposed by Nick Szabo in 1994, have become one of the most effective features of Ethereum [44]. Smart contract programs for blockchain are designed to establish access rights and various policies. For instance, a rule might be set specifying that devices automatically switch to energy-saving mode when the meter hits 135 KW [33,51,64]. The Internet of Things (IoT) is a rapidly advancing technology due to the growth of high-speed networks and smart devices. However, IoT devices are particularly vulnerable to attacks and cannot defend themselves. In this context, we explore various characteristics of blockchain networks, such as Proof of Work (POW), decentralization, persistence, and network scalability [45,58]. We also examine the challenges faced by IoT devices, including data integrity, access control, and privacy, while presenting blockchain-based solutions proposed in the literature.

7.6. Consensus Protocols/Algorithms in Blockchain

Consensus algorithms are designed to securely update replicated shared states, which are essential for the functioning of blockchain principles [39]. One such system is state machine replication, a consensus protocol that ensures all replicas of the shared state are synchronized and in agreement at any given point [39,61,63,69]. Consensus protocols incentivize participating nodes to create and add new blocks to the blockchain [34,45,56,64]. These protocols must demonstrate Byzantine Fault Tolerance (BFT) properties. They are typically categorized as proof of a given delegation, forming the basis of these algorithms in selecting a leader [52,61,69]. Figure 20 shows different types of consensus algorithms.

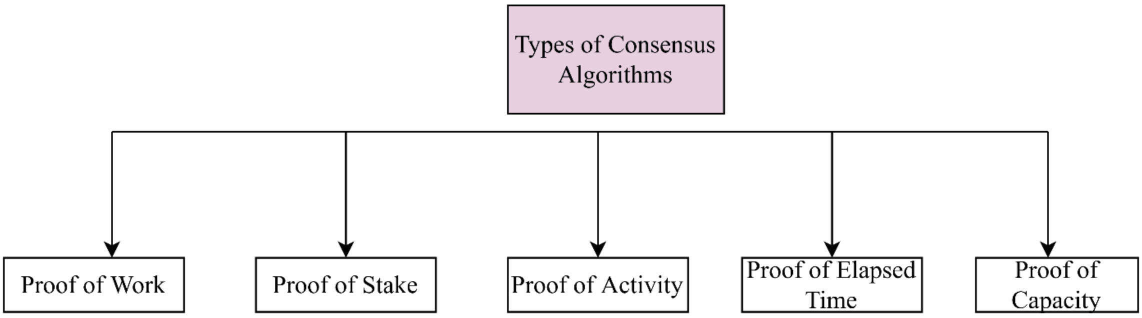

Figure 20. Most popular consensus algorithms.

- The proof-of-work (PoW) algorithm is computed as a mathematical problem. The existence of PoW makes it possible to talk about blockchain today [52,61]. PoW is considered hard, computationally heavy, and expensive in terms of energy consumption [34,52]. PoW is often considered challenging because it is not easy to obtain a value for Bitcoin or another cryptocurrency because of the performed work. One of the main goals of PoW is to avoid spamming attacks. A PoW proof should be an asymmetric task that is hard to solve but easy to verify. Thus, a miner requires much more time to find the nonce that solves the hash problem, while other miners in the network can easily verify and validate the solution [45,52,63]. One of the main problems of PoW [52,61,68,69] is that multiple miners working on a standard objective lead to tremendous wastage of computing power and electricity. With a high requirement of computing power, mining has advantages if done in pools; however, this defeats the goal of decentralization. PoW-based consensus is vulnerable when a user takes control of 51 percent of processing power in the network, as illustrated in Figure 21, [39,45,61].

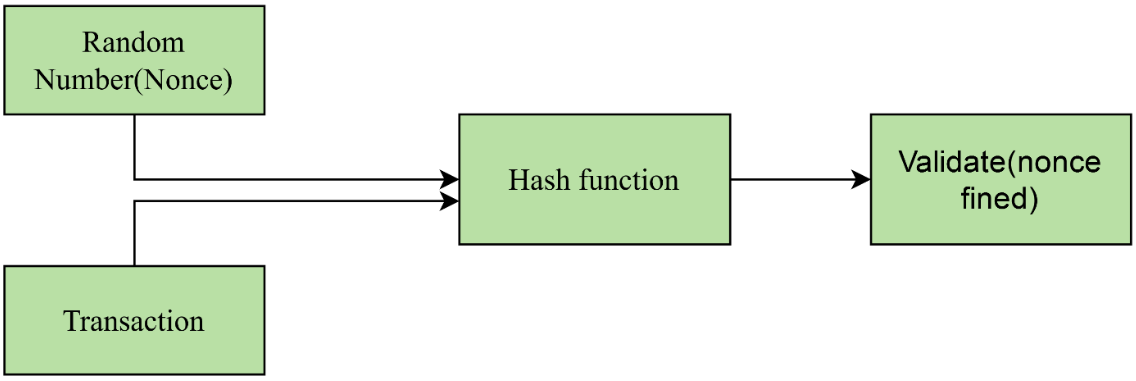

Figure 21. Proof of work transaction structure.

- In proof-of-stake (PoS), the main concept is the "stake". Nodes participating in this consensus process lock a specific number of coins in their account. The idea is to ensure that every node acts respecting the protocol rules and does not deviate from them [34,45,56]. As a result, users with larger stakes have a stronger incentive to protect the system's reliability, as they risk losing more if the stake is compromised. Thus, there is less chance of a node becoming malicious. It has been stated that PoS protocols have low performance; for this reason, a few other variations from Algorand have been proposed on top of the Byzantine agreement [56,61,68]. See Figure 22 for how these transactions work.

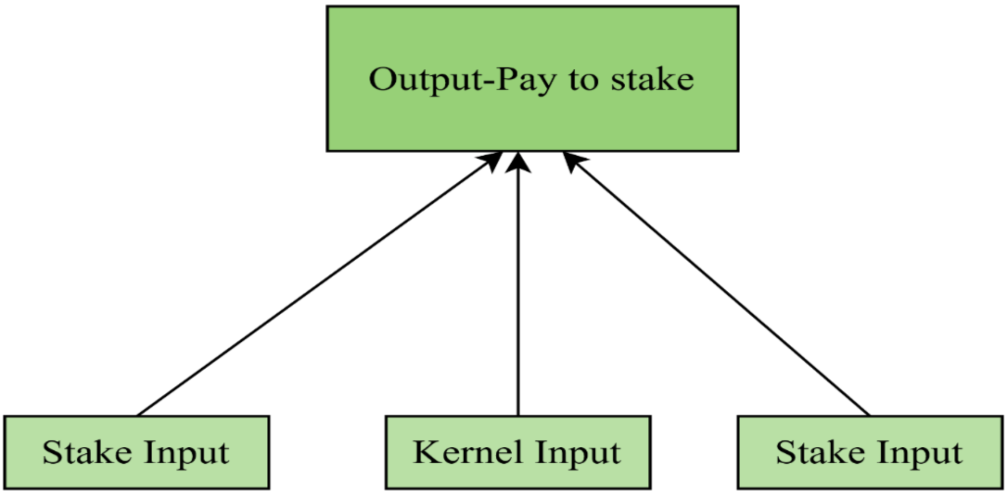

Figure 22. Proof-of-stake transaction structure.

- Algorand solves the decentralization, scalability, and security by attaching a cryptographic proof where each new block checks the eligibility of the block proposed to be chosen, which is directly proportional to its stake. Based on security and performance, Algorand can tolerate malicious behavior and provide high scalability [34,56,63,69]. As part of PoS, Delegated PoS requires voting to reach a consensus [52,61,68]. Network management responsibilities are assigned to delegates who do not receive incentives. Their duties include fee schedules, block intervals, and transaction sizes. Changes can also be adopted based on the network's voting. Proof-of-authority (POA) is the successor of PoS, where the reputation of the validator acts as a stake [52,63]. When it comes to reputation, it is hard to regain when lost; thus, why there are better choices to use as the stake. PoA networks have high throughput but are centrally controlled by the validators [34,52,56,60]. Figure 23 shows the structure of a hybrid network combining both proof-of-work and proof-of-stake.

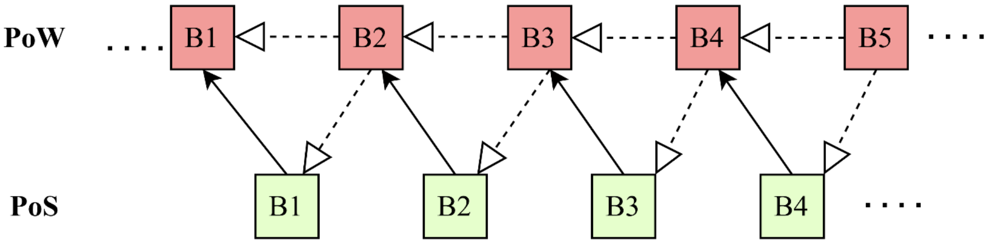

Figure 23. Transaction structure combining proof-of-work and proof-of-stake.

- Proof-of-activity was introduced as an alternative to Bitcoin mining and combines elements of both proof-of-work and proof-of-stake to achieve consensus. Its primary aim is to reward stakeholders who are actively involved in the network [39,60,68,69]. Additionally, proof-of-activity is used to ensure distributed consensus by finding proof-of-work against an empty block with no transactions included. From there, a group of validators is selected to vote on the validity of the mined block header [39,61].
- Proof of elapsed time (PoET) is designed to eliminate the computational power requirements of PoW-based consensus protocols. Implemented in the Sawtooth platform, this protocol addresses the Byzantine agreement problem using a lottery-like approach to ensure fairness, investment, and verification during leader election [39,45,56,69]. In PoET, peers wait for a random amount of time to elapse; the peer that finishes waiting first is selected as the leader to create a new block [56,61,63]. This process takes place in a secure memory area such as Intel's SGX, which is commonly used in the Sawtooth platform [56,60].
- Proof-of-capacity (PoC) offers an alternative to PoW by utilizing miners' hard drive space to solve cryptographic challenges rather than their computational power. In PoC, miners use a technique called "plotting" to pre-store potential solutions to problems, eliminating the need for real-time calculations. This approach is more energy-efficient than PoW [45,52,56,69]. However, there is a risk that multiple users could collaborate to pool their storage resources within a centralized network.
- The Kafka protocol utilizes a shared subscribe messaging pattern capable of transferring large volumes of log data with minimal latency. It involves producers, topics, consumers, and brokers. Producers publish recorded information as a stream of messages, which are segments of partitioned files [56,60,63,68]. These messages are stored by brokers in the latest segment file and subscribed consumers can read them by requesting access from the brokers [56,61]. Kafka uses a Crash Fault Tolerant (CFT) consensus protocol, which can handle up to 50 percent of network failures and is primarily implemented in fabric systems [45,69].
- The Practical Byzantine Fault Tolerance (PBFT) protocol is a widely recognized protocol that has gained increased attention with the rise of Blockchain technology. PBFT operates under the assumption that less than 33 percent of network nodes behave maliciously. Consensus is achieved through three phases: pre-prepare, prepare, and commit [56,60,68]. In this process, each node acts as a validating replica that votes to elect a primary node, or leader, which initiates the three-phase consensus after receiving a request from clients [34,39,56,69]. The process starts by multicasting a pre-prepared message. Despite its effectiveness, PBFT lacks scalability, as it supports only a limited number of nodes and requires the transfer of numerous messages to reach consensus [56].
- The Ripple Protocol Consensus Algorithm (RPCA) was designed to ensure security and stability within a cryptocurrency-based network for remittance transfers without the need to implement smart contracts [61,63]. Each node in RPCA maintains a

unique list consisting of a set of trusted validator nodes involved in the consensus process [34,45,56]. The nodes listen to these trusted validators; if consensus is not achieved on a set of transactions, then the nodes' proposals are adjusted according to suggestions from the trusted validators [56,60,68,69]. Transactions that receive more than 80 percent positive votes are processed, while others are either discarded or placed in a candidate pool for future ledger inclusion [56,63].

- The Stellar Consensus Protocol (SCP) operates as a Federated Byzantine Agreement (FBA). Unlike other protocols, SCP does not require consensus from a majority of nodes in the network; instead, each node selects a subset of trusted nodes within the network [45,52]. Decisions are made based on the consensus of these trusted nodes, and any misbehaving nodes are excluded from both the trusted group and the decision-making process. In Hyperledger Fabric, which uses PBFT, network nodes validate each transaction and a leader is chosen to propose the transaction sequence. The Delegated Byzantine Fault Tolerant (DBFT) protocol, on the other hand, designates specific nodes to reach consensus on the next block to be added to the blockchain [52,60,68,69]. These nodes, referred to as bookkeepers, vote continuously and are selected through a registration process within the network [34,52] The table below provides a comprehensive overview of different consensus algorithms.

Overall, the various consensus mechanisms impact IoT-blockchain integration differently, particularly as concerns efficiency, security, and resource consumption. Proof-of-work (PoW), known for its robust security, is computationally intensive, which can be a constraint for IoT networks with limited resources. In contrast, proof-of-stake (PoS) reduces energy consumption by selecting validators based on stake rather than computation, making it feasible for IoT applications where power efficiency is crucial. Practical Byzantine Fault Tolerance (PBFT) offers another suitable option, as it minimizes latency and is particularly effective in low-resource environments thanks to its low computational requirements. This analysis suggests that while PoW may offer stronger security, PoS, and PBFT are better aligned with the efficiency and scalability demands of IoT systems.

7.7. Taxonomy of Security Research in IoT

In this subsection, we provide more information about the general taxonomy of security research related to the IoT domain. We discuss this by separating the topic into domain security for IoT in the following areas: developing authorized schemes, ensuring trust, preventing attacks, designing authentication protocols, privacy, secure data management, and ensuring basic security [42,60,67].

The above categories are integrated into the IoT security domain. Authentication protocols are designed to authenticate users and devices; even the simplest cryptographic operations are connected to data authentication. One area where authentication is used consists of biometric-based solutions; interestingly, user authentication is also involved in blockchain-based fingerprint verification methods [33,42,67]. Data authentication is also considered when designing signing schemes to suit different applications. In addition, smart contracts can be deployed on blockchains to develop appropriate authorization schemes [42,60]. Another aspect of IoT security is cyberattacks, which represent a serious threat to IoT systems. In particular, damage to industrial IoT systems can disrupt data due to attacks such as replay, DDoS, and other attack types. This topic requires further analysis, as many studies and solutions have found different explanations for these attacks [42,60].

Concerning IoT, data and user privacy are essential and crucial requirements for all devices. Different kinds of blockchains have proposed various solutions, such as data aggregation techniques to preserve privacy. In addition, secure data management is an essential concern that many researchers are focusing on [33,42,67]. One well-known solution is securing data management by multi-key aggregate keyword searchable encryption. When it comes to security, one real solution is CIA security, non-repudiation, and access control [42,60,67]. Other solutions that have been proposed include using SVM, credit-based consensus mechanisms, and various blockchain-based encryption techniques [42].

Moreover, consensus algorithms and re-encryption techniques have been proposed to ensure trust in blockchains. The figure below shows the taxonomy of security research advancements in IoT, helping to illustrate areas that different researchers have focused on and what solutions have been proposed. An in-depth analysis can aid in identifying solutions to various security issues [33,42].

8. Research Directions and Open Research Issues of IoT with Blockchain

Blockchain is a powerful and emerging technology. While the integration of IoT with blockchain presents numerous benefits, it also brings several challenges that need to be addressed in order to fully unlock the potential of both technologies. In light of the current security concerns surrounding blockchain systems, we highlight future trends to encourage further research in this area. To make these solutions practical, specific research challenges must be overcome to make blockchain a viable option for securing IoT data and integrating blockchain with IoT [56,58,59]. Figure 24 outlines the open research areas for future exploration. This section delves into these challenges, the tradeoffs between public and private blockchain implementations, and potential research directions for blockchain–IoT integration. In the IoT sector, the ideal distributed platform should support the following key functionalities:

- Trustless peer-to-peer M2M communication;
- Decentralized access control;
- Private-by-design file sharing;
- Scalable security provision over multiple IoT use cases.

- Security: IoT systems are often seen as easy targets for various security attacks due to the inadequate security measures in place for billions of heterogeneous Internet of Things devices [64]. Advanced encryption algorithms are often not feasible for IoT devices. Blockchain technology also faces security vulnerabilities, such as bugs in smart contracts and attacks on decentralized autonomous organizations (DAOs) [4,79–82]. Because blockchain data are stored in a public ledger, privacy and confidentiality issues remain. However, different anonymization or encryption techniques can be applied to protect this information. An effective IoT network should be resilient against all potential attacks. Current advanced security strategies largely rely on complex hash puzzles, making it challenging to secure a network with resource-limited devices that cannot handle heavy computational tasks [34,54,64]. Therefore, further research is needed to address the security challenges in both IoT and Blockchain.
- Scalability: A key challenge in integrating blockchain with IoT is the ability of blockchain to scale and operate effectively within large-scale networks such as IoT. Due to scalability limitations in existing blockchains, IoT systems cannot fully leverage them because of slow transaction speeds and the high volume of concurrent workloads [45,51,56,58]. Blockchain technology is currently facing significant scalability issues. While proposals to address these challenges have been put forward, such as developing more scalable consensus algorithms and creating private Blockchains for IoT, additional research is needed to find efficient solutions [56]. Two potential approaches to improve blockchain scalability in IoT are (1) designing more scalable consensus algorithms, and (2) building private or consortium blockchains specifically for IoT. Improving scalability in current implementations may affect throughput and latency. More details can be found in Table 8.
- IoT Edge Device Constraints: IoT smart devices are interconnected to automate processes; however, many of these devices face strict computational and networking limitations, which creates challenges when implementing blockchain-based decentralized systems [79,83]. Despite these constraints, blockchain technology can manage both structured and unstructured data transfers through distributed records, facilitating interoperability across various IoT edge devices [4,81,84]. One proposed solution to extend blockchain to the IoT edge is to utilize computationally capable IoT gateways for end-to-end communication, leveraging their high performance and networking

capabilities. A key challenge in this approach is to enable IoT devices and gateways to transmit transactions to the blockchain using light clients without establishing centralized block validation pools [72,85].

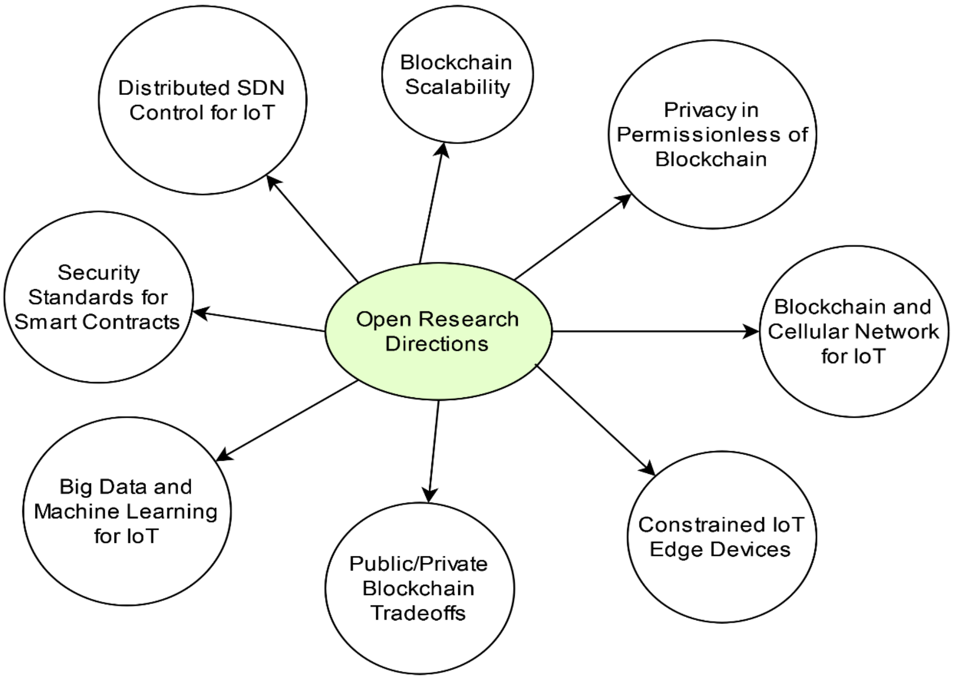
Distributed SDN Control for IoT
Blockchain Scalability
Privacy in Permissionless of Blockchain
Security Standards for Smart Contracts
Open Research Directions
Blockchain and Cellular Network for IoT
Big Data and Machine Learning for IoT
Public/Private Blockchain Tradeoffs
Constrained IoT Edge Devices

Figure 24. Open research directions.

Table 8. Expected data size with increase in transaction throughput.

Block Size	Block Fees	TPS	Annual Size
1	0.12 BTC	1	15 GB
0.9 MB	0.36 BTC	3	47 GB
3 MB	1.2 BTC	10	150 GB
30 MB	12 BTC	100	1.5 TB
300 MB	120 BTC	1000	15 TB
3 GB	1200 BTC	10,000	150 TB
30 GB	12,000 BTC	100,000	1500 TB

- Smart Contract-Related Solutions: Ethereum supports multiple programming languages, with Solidity being the most commonly used for writing and compiling smart contracts. Smart contracts, first introduced by Nick Szabo in 1994, are a key feature of Ethereum's efficiency [4]. Blockchain research-IoT integration includes developing security standards for smart contracts to ensure that their security is not compromised by vulnerabilities that avoid blockchain's inherent security features. For instance, DAO attacks highlight how adversaries can exploit weaknesses in smart contracts [4,81,82,86]. Therefore, smart contracts must securely model the application logic of IoT systems. To do this, they rely on data feeds from real-world systems known as oracles, which provide reliable real-world data. Given the potential unreliability of IoT devices, validating these smart contracts can be challenging [8,81]. Blockchain technologies face design constraints in transaction capacity, validation protocols, and smart contract implementation [86]. Thus, future research is crucial to enhancing the use of smart contracts in IoT applications.

- Data Storage: While blockchain and IoT data storage frameworks handle various types of information, the primary challenge is the systematic sharing and securing of this critical data. In blockchain design, there are two main components, namely, transaction hubs and linked blocks. The blockchain framework provides users with accountability, privacy, and traceability [72,80,84]. User data are stored in blocks corresponding to specific block numbers, which are used to identify the user only at designated thresholds. The data volume is verified by referencing a specific block number and its segmentation.
  The data packets received are initially stored in blocks by users during the first checkpoint along with the fragmentation of the stored data, as illustrated in Table 8, which shows that the size of the data increases with the volume of transactions. The new cluster number is then encrypted using a shared key derived from the Diffie–Hellman algorithm. This encryption ensures that the cluster number's owner cannot be determined by others. Because partitions are crash-resistant and only the legitimate user knows the cluster number, unauthorized users are prevented from accessing the data [72,84,85]. Although data storage frameworks for blockchain IoT (BIoT) handle diverse information assets, the main challenges involve systematically sharing and securing these crucial data [87]. Therefore, extensive research is needed to enhance the security of data storage for blockchain and IoT devices [86].
- SDN Integration for the Blockchain-Based IoT Edge: Fog computing, also known as edge computing, is an extensive virtual system that facilitates processing and storage between users and traditional cloud data centers [4,80,88,89]. In the evolving landscape of the internet, particularly the IoT, software-defined networking (SDN) and network function virtualization (NFV) are designed to provide a virtualized edge platform where virtual hosts can be dynamically deployed [4,84]. SDN's separation of the control plane and data forwarding functions allows for easy management and control of virtual IoT resources. This approach has the potential to improve IoT edge configuration and management. However, as SDN and NFV technologies advance, they introduce new cybersecurity challenges, which are further complicated when integrated with IoT.
- Big Data and Machine Learning for Decentralized IoT Frameworks: In the IoT, machine learning can be used to make intelligent decisions to optimize automation tasks such as scheduling, managing IoT assets, and energy transactions [4,84,87,90]. The secure and verifiable blockchain structure can be used to ease extensive data management. However, data analytics using blockchain structure implies too much overhead. Despite this, processing all transactions will not be necessary in most cases; hence, intermediate or efficient auxiliary systems may be implemented to increase overall efficiency. In addition, blockchain-based architectures for ample data storage already exist [79]. IoT–blockchain integration will significantly increase the use of blockchain technology, and will establish cryptocurrencies on the same level as current fiduciary money. One of the significant concerns about blockchain, particularly cryptocurrencies, is their volatility, which individuals have exploited for profit [82]. The mixture of blockchain and IoT suggests a robust methodology that can meaningfully open the path for new business methods and applications [78,88,89]. Additionally, the design of blockchain for IoT applications would need to adapt to the specific properties of IoT networks, such as their immense scale, inherent partitioning, incomplete network connectivity, non-trivial topology, non-zero propagation delay, heterogeneous data, and finite device memory [91].

In addition, future research could explore the specific questions of how to optimize low-latency consensus protocols for resource-constrained IoT devices and which frameworks can best evaluate the security scalability of blockchains in high-density IoT networks. Answering these questions could pave the way for practical and scalable IoT solutions capable of supporting real-time data requirements. In addition, it would be possible to create a framework for evaluating IoT–blockchain integrations in terms of the latency, security level, and resource consumption of IoT devices.

9. Conclusions

This survey makes a unique contribution by providing a comprehensive taxonomy of security and integration challenges at the intersection of IoT and blockchain technology. While previous studies have primarily addressed blockchain and IoT individually, this paper focuses on the integration of these technologies, identifying critical areas such as protocol feasibility and resource constraints. Thus, this work adds depth to the field by analyzing consensus protocols specifically through the lens of IoT constraints, thereby offering a resource for researchers and practitioners to further develop secure and efficient IoT–blockchain solutions. Although there are promising implications, challenges such as scalability, energy consumption, and data privacy need to be addressed. The Internet of Things continues to proliferate, and security and privacy remain paramount concerns. This survey has explored the compelling solutions provided by integrating blockchain technology into the IoT to mitigate these concerns. We have investigated the characteristics and components of blockchain technology, examined its possible applications in IoT contexts, and discussed architectures for IoT–Blockchain integration. Furthermore, we have highlighted the importance of blockchain in protecting IoT networks from cyberattacks while providing practical suggestions and outlining the consensus protocols and algorithms inherent to the technology. Future research should focus on optimizing blockchain for IoT environments, developing robust consensus algorithms, and establishing interoperability standards. By addressing these challenges, the integration of blockchain and IoT can significantly contribute to secure, efficient, and scalable systems for various applications.

Author Contributions: Conceptualization, M.A.O. and K.T.; methodology, M.A.O., M.R., and M.A. (Meryem Abouali); formal analysis, M.A. (Meryem Abouali) and M.A. (Mohammed Alja'afreh); investigation, M.R., M.A. (Meryem Abouali), K.T., and A.K.; resources, M.A. (Mohammad Alja'afreh) and A.K.; writing—original draft preparation, M.R., K.T., M.A. (Meryem Abouali), and A.K.; writing—review and editing, M.A.O. and M.A. (Meryem Abouali); visualization, A.K.; project administration, M.A.O. All authors have read and agreed to the published version of the manuscript

Funding: This research received no external funding

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Kumar, J.S.; Patel, D. A Survey on Internet of Things: Security and Privacy Issues. *Int. J. Comput. Appl.* **2014**, *90*, 20–26. [CrossRef]
2. Khalil, K.; Elgazzar, K.; Abdelgawad, A.; Bayoumi, M. A Security Approach for CoAP-based Internet of Things Resource Discovery. In Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2–16 June 2020. [CrossRef]
3. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* **2015**, 17, 2347–2376. [CrossRef]
4. Lone, A.H.; Naaz, R. Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic review of the literature. *Comput. Sci. Rev.* **2021**, *39*, 100360. [CrossRef]
5. Davis, K. *The Urbanization of the Human Population, Book "The City Reader"*, 5th ed.; Sicentific American: New York, NY, USA, 2011; Volume 5, pp. 20–30. ISBN 9780203869260.
6. Wardana, A.A.; Perdana, R.S. Access Control on Internet of Things based on Publish/Subscribe using Authentication Server and Secure Protocol. In Proceedings of the 2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE), Bali, Indonesia, 24–26 July 2018; pp. 118–123. [CrossRef]
7. Ragothaman, K.; Wang, Y.; Rimal, B.; Lawrence, M. Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions. *Sensors* **2023**, *23*, 1805. [CrossRef]
8. Obaidat, M.; Khodiaeva, M.; Obeidat, S.; Salane, D.; Holst, J. Security Architecture Framework for Internet of Things. In *10th IEEE Ubiquitous Computing, Electronics and Mobile Communication Conference*; Columbia University: New York, NY, USA, 2019.
9. Marr, B. 2024 IoT and Smart Device Trends What You Need to Know for the Future. Forbes. 2023. Available online: https://www.forbes.com/sites/bernardmarr/2023/10/19/2024-iot-and-smart-device-trends-what-you-need-to-know-for-the-future/ (accessed on 19 October 2023).

10. Bezabih, Y.M.; Mequanint, A.; Alamneh, E.; Bezabih, A.; Sabiiti, W.; Roujeinikova, A.; Bezabhe, W.M. Correlation of the global spread of coronavirus disease-19 with atmospheric air temperature. *medRxiv* **2020**, *preprint*.
11. Abouali, M.; Sharma, K.; Saadawi, T. Access Delegation Framework for Private Decentralized Patient Health Records Sharing System Based on Blockchain. In Proceedings of the 2022 IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2022; pp. 7–13.
12. Fabiano, N. The Internet of Things ecosystem: The Blockchain and privacy issues. The challenge for a global privacy standard. In Proceedings of the 2017 International Conference on Internet of Things for the Global Community (IoTGC), Funchal, Portugal, 10–13 July 2017.
13. Wang, T.; Zheng, Z.; Rehmani, M.H.; Yao, S.; Huo, Z. Privacy preservation in big data from the communication perspective—A survey. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 753–778. [CrossRef]
14. Rivera, R.; Robledo, J.G.; Larios, V.M.; Avalos, J.M. How digital identity on Blockchain can contribute in a smart city environment. In Proceedings of the 2017 International Smart Cities Conference (ISC2), Wuxi, China, 14–17 September 2017.
15. Sahu, S.K.; Mazumdar, K. Exploring security threats and solutions Techniques for Internet of Things (IoT): From vulnerabilities to vigilance. *Front. Artif. Intell.* **2024**, *7*, 1397480. [CrossRef]
16. Yang, S.; Long, X.A.; Peng, H.; Gao, H. Optimization of heterogeneous clustering routing protocol for internet of things in wireless sensor networks. *J. Sens.* **2022**, *2022*, 4327414. [CrossRef]
17. De Montjoye, Y.A.; Shmueli, E.; Wang, S.S.; Pentl, A.S. openpds: Protecting the privacy of metadata through safeanswers. *PLoS ONE* **2014**, *9*, e98790. [CrossRef]
18. Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Internet Things J.* **2018**, *5*, 1184–1195. [CrossRef]
19. Abouali, M.; Sharma, K.; Saadawi, T. Blockchain-Based Solution for Patient Controlled Health Records Sharing for Private Decentralized Storage. In *Advanced AI and Internet of Health Things Technologies for Combating Pandemic*; Springer: Berlin/Heidelberg, Germany, 2023; eBook ISBN 978-3-031-28631-5; Print ISBN978-3-031-28630-8.
20. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Satoshi Nakamoto* **2008**, 21260. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 19 November 2024).
21. Khordadpour, P.; Ahmadi, S. Security and Privacy Enhancing in Blockchain-based IoT Environments via Anonym Auditing. *arXiv* **2024**, arXiv: 2403.01356
22. Pilkington, M. Blockchain Technology: Principles and applications. In *Research Handbook on Digital Transformations*; Edward Elgar Publishing: Northampton, MA, USA, 2016; pp. 225–253.
23. Morgan, J.P. Quorum, Advancing Blockchain Technology. 2018. Available online: https://www.youtube.com/watch?v=mUr8cGZprSI (accessed on 19 November 2024).
24. Anees, T.; Habib, Q.; Al-Shamayleh, A.S.; Khalil, W.; Obaidat, M.A.; Akhunzada, A. The Integration of WoT and Edge Computing: Issues and Challenges. *Sustainability* **2023**, *15*, 5983. [CrossRef]
25. Kaswan, M.S.; Chaudhary, R.; Garza-Reyes, J.A.; Singh, A. A review of Industry 5.0: From key facets to a conceptual implementation framework. *Int. J. Qual. Reliab. Manag.* **2024**. [CrossRef]
26. Fernández-Caramés, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* **2018**, *6*, 32979–33001. [CrossRef]
27. Krco, S.; Cleary, D.; Parker, D. P2P mobile sensor networks. In Proceedings of the 38th Annual Hawaii International Conference on System Sciences, Big Island, HI, USA, 6 January 2005.
28. Seok, B.; Park, J.; Park, J.H. A lightweight hash-based Blockchain architecture for industrial IoT. *Appl. Sci.* **2019**, *9*, 3740. [CrossRef]
29. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
30. Aljabhan, B.; Obaidat, M.A. Privacy-Preserving Blockchain Framework for Supply Chain Management: Perceptive Craving Game Search Optimization (PCGSO). *Sustainability* **2023**, *15*, 6905. [CrossRef]
31. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A survey on privacy protection in Blockchain system. *J. Netw. Comput. Appl.* **2019**, *126*, 45–58. [CrossRef]
32. Lo S.K.; Liu, Y.; Chia, S.Y.; Xu, X.; Lu, Q.; Zhu, L.; Ning, H. Analysis of Blockchain solutions for IoT: A systematic literature review. *IEEE Access* **2019**, *7*, 58822–58835. [CrossRef]
33. Dai, H.N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A Survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [CrossRef]
34. Wu, M.; Wang, K.; Cai, X.; Guo, S.; Guo, M.; Rong, C. A comprehensive survey of Blockchain: From theory to IoT applications and beyond. *IEEE Internet Things J.* **2019**, *6*, 8114–8154. [CrossRef]
35. Da Xu, L.; He, W.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243.
36. Kumar, U.; Kaswan, M.S.; Kumar, R.; Chaudhary, R.; Garza-Reyes, J.A.; Rathi, R.; Joshi, R. A systematic review of Industry 5.0 from main aspects to the execution status. *TQM J.* 2023, *ahead-of-print*.
37. Khan, M.A.; Salah, K. IoT security: Review, Blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
38. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet Things J.* **2019**, *6*, 2188–2204. [CrossRef]

39. Makhdoom, I.; Abolhasan, M.; Abbas, H.; Ni, W. Blockchain's adoption in IoT: The challenges, and a way forward. *J. Netw. Comput. Appl.* **2019**, *125*, 251–279. [CrossRef]
40. Muhammad Salek Ali; Massimo Vecchio; Miguel Pincheira; Koustabh Dolui; Fabio Antonelli; Mubashir Husain Rehmani. Applications of Blockchains in the Internet of Things: A comprehensive survey. *IEEE Commun. Surv. Tutorials* **2018**, *21*, 1676–1708.
41. Yang, R.; Yu, F.R.; Si, P.; Yang, Z.; Zhang, Y. Integrated Blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1508–1532. [CrossRef]
42. Viriyasitavat, W.; Da Xu, L.; Bi, Z.; Hoonsopon, D. Blockchain technology for applications in internet of things—Mapping from system design perspective. *IEEE Internet Things J.* **2019**, *6*, 8155–8168. [CrossRef]
43. Sengupta, J.; Ruj, S.; Bit, S.D. A comprehensive survey on attacks, security issues and Blockchain solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
44. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R. A systematic literature review of Blockchain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [CrossRef]
45. Abouali, M.; Sharma, K.; Ajayi, O.; Saadawi, T. Blockchain Framework for Secured On-Demand Patient Health Records Sharing. In Proceedings of the 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 1–4 December 2021; pp. 35–40.
46. Peters, M.D.J.; Godfrey, C.M.; Khalil, H.; McInerney, P.; Parker, D.; Soares, C.B. Guidance for conducting systematic scoping reviews. *Int. Evid. Based Healthc.* **2015**, *13*, 141–146. [CrossRef] [PubMed]
47. Atlam, H.F.; Azad, M.A.; Alzahrani, A.G.; Wills, G. A Review of Blockchain in Internet of Things and AI. *Big Data Cogn. Comput.* **2020**, *4*, 28. [CrossRef]
48. Kumar, R.L.; Khan, F.; Kadry, S.; Rho, S. A survey on Blockchain for industrial internet of things. *Alex. Eng. J.* **2022**, *61*, 6001–6022. [CrossRef]
49. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. A survey on the adoption of Blockchain in iot: Challenges and solutions. *Blockchain Res. Appl.* **2021**, *2*, 100006. [CrossRef]
50. Tran, N.K.; Babar, M.A.; Boan, J. Integrating Blockchain and Internet of Things systems: A systematic review on objectives and designs. *J. Netw. Comput. Appl.* **2021**, *173*, 102844. [CrossRef]
51. Nasir, M.H.; Arshad, J.; Khan, M.M.; Fatima, M.; Salah, K.; Jayaraman, R. Scalable Blockchains—A systematic review. *Future Gener. Comput. Syst.* **2022**, *126*, 136–162. [CrossRef]
52. Sadawi, A.; Hassan, A.M.S.; Ndiaye, M.J.I.A. A survey on the integration of Blockchain with IoT to enhance performance and eliminate challenges. *IEEE Access* **2021**, *9*, 54478–54497. [CrossRef]
53. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and iot integration: A systematic survey. *Sensors* **2018**, *18*, 2575. [CrossRef]
54. Al-Megren, S.; Alsalamah, S.; Altoaimy, L.; Alsalamah, H.; Soltanisehat, L.; Almutairi, E. Blockchain use cases in digital sectors: A review of the literature. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018.
55. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on Blockchain for Internet of Things. *Comput. Commun.* **2019**, *136*, 10–29. [CrossRef]
56. Sultan, A.; Malik, M.S.A.; Mushtaq, A. Internet of Things security issues and their solutions with Blockchain technology characteristics: A systematic literature review. *Am. J. Compt. Sci. Inform. Technol.* **2018**, *6*, 27. [CrossRef]
57. Brotsis, S.; Limniotis, K.; Bendiab, G.; Kolokotronis, N.; Shiaeles, S. On the suitability of Blockchain platforms for IoT applications: Architectures, security, privacy, and performance. *Comput. Netw.* **2021**, *191*, 108005. [CrossRef]
58. Jesus, E.F.; Chicarino, V.R.; De Albuquerque, C.V.; Rocha, A.A.D.A.A. survey of how to use Blockchain to secure Internet of things and the stalker attack. *Secur. Commun. Netw.* **2018**, 2018, 9675050. [CrossRef]
59. Butun, I.; Osterberg, P. A review of distributed access control for Blockchain systems towards securing the internet of things. **2020**, *9*, 5428–5441.
60. Alamri, M.; Jhanjhi, N.Z.; Humayun, M. Blockchain for Internet of Things (IoT) research issues challenges & future directions: A review. **2019**, *19*, 244–258.
61. Da Xu, L.; Lu, Y.; Li, L. Embedding Blockchain technology into IoT for security: A survey. *IEEE Internet Things J.* **2021**, *8*, 10452–10473.
62. Salimitari, M.; Chatterjee, M.; Fallah, Y.P. A survey on consensus methods in Blockchain for resource-constrained IoT networks. *Internet Things* **2020**, *11*, 100212. [CrossRef]
63. Uddin, M.; Selvarajan, S.; Obaidat, M.; Arfeen, S.U.; Khadidos, A.O.; Khadidos, A.O.; Abdelhaq, M. From Hype to Reality: Unveiling the Promises, Challenges and Opportunities of Blockchain in Supply Chain Systems *Sustain. J.* **2023**, *15*, 12193. [CrossRef]
64. Patil, P.; Sangeetha, M.; Bhaskar, V. Bhaskar, Blockchain for IoT access control, security and privacy: A review. **2021**, *117*, 1815–1834.
65. Huo, R.; Zeng, S.; Wang, Z.; Shang, J.; Chen, W.; Huang, T.; Wang, S.; Yu, F.R.; Liu, Y. A comprehensive survey on Blockchain in industrial internet of things: Motivations, research progresses, and future challenges. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 88–122. [CrossRef]

66. Ali, J.; Ali, T.; Alsaawy, Y.; Khalid, A.S.; Musa, S. Blockchain-based smart-IoT trust zone measurement architecture. In Proceedings of the International Conference on Omni-Layer Intelligent Systems, Crete, Greece, 5–7 May 2019; pp. 152–157.
67. Pieroni, A.; Scarpato, N.; Felli, L. Blockchain and IoT convergence—A systematic survey on technologies, protocols and security. *Appl. Sci.* **2020**, *10*, 6749. [CrossRef]
68. Kumar, R.; Sharma, R. Leveraging Blockchain for Ensuring Trust in IoT: A Survey. *J. King Saud-Univ. Comput. Inf. Sci.* **2022**, *34*, 8599–8622. [CrossRef]
69. Lao, L.; Li, Z.; Hou, S.; Xiao, B.; Guo, S.; Yang, Y. A survey of IoT applications in Blockchain systems: Architecture, consensus, and traffic modeling. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–32. [CrossRef]
70. Reyna, A.; Martin, C.; Chen, J.; Soler, E.; Diaz, M. On Blockchain and its integration with IoT. *Challenges Oppor.* **2018**, *88*, 173–190.
71. Abouali, M.; Sharma, K.; Ajayi, O.; Saadawi, T. Performance Evaluation of Secured Blockchain-Based Patient Health Records Sharing Framework. In Proceedings of the 2022 IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 1–4 June 2022.
72. Noby, D.A.; Khattab, A. A survey of Blockchain applications in IoT systems. In Proceedings of the 2019 14th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 17 December 2019.
73. Shehzad, K.; Afrasayab, M.; Khan, M.; Mushtaq, M.A.; Ahmed, R.L.; Saleemi, M.M. Use of Blockchain in Internet of things: A systematic literature review. In Proceedings of the 2019 Cybersecurity and Cyberforensics Conference (CCC), Melbourne, VIC, Australia, 8–9 May 2019.
74. Khor, J.H.; Sidorov, M.; Woon, P.Y. Public Blockchains for resource-constrained iot devices—A state-of-the-art survey. *IEEE Internet Things J.* **2021**, *8*, 11960–11982. [CrossRef]
75. Moin, S.; Karim, A.; Safdar, Z.; Safdar, K.; Ahmed, E.; Imran, M. Securing IoTs in distributed Blockchain: Analysis, requirements and open issues. *Future Gener. Comput. Syst.* **2019**, *100*, 325–343. [CrossRef]
76. Mohanta, B.K.; Jena, D.; Satapathy, U.; Patnaik, S. Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and Blockchain technology. *Internet Things* **2020**, *11*, 100227. [CrossRef]
77. Anand, M.V.; Vijayalakshmi, S. A Survey on Blockchain Adaptability in IoT Environments. In Proceedings of the 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 4–5 March 2021.
78. Kumari, A.; Gupta, R.; Tanwar, S. Amalgamation of Blockchain and IoT for smart cities underlying 6G communication: A comprehensive review. *Comput. Commun.* **2021**, *172*, 102–118. [CrossRef]
79. Ferrag, M.A.; Shu, L.; Yang, X.; Derhab, A.; Maglaras, L. Security and privacy for green IoT-based agriculture: Review, Blockchain solutions, and challenges. *IEEE Access* **2020**, *8*, 32031–32053. [CrossRef]
80. Azbeg, K.; Ouchetto, O.; Andaloussi, S.J.; Fetjah, L. A taxonomic review of the use of IoT and Blockchain in healthcare applications. *IRBM* **2022**, *43*, 511–519. [CrossRef]
81. Liang, W.; Ji, N. Privacy challenges of IoT-based Blockchain: A systematic review. *Clust. Comput.* **2022**, *25*, 2203–2221. [CrossRef]
82. Chowdhury, M.J.M.; Ferdous, M.S.; Biswas, K.; Chowdhury, N.; Muthukkumarasamy, V. A survey on Blockchain-based platforms for IoT use-cases. *Knowl. Eng. Rev.* **2020**, *35*, e19. [CrossRef]
83. Chen, F.; Xiao, Z.; Cui, L.; Lin, Q.; Li, J.; Yu, S. Blockchain for Internet of things applications: A review and open issues. *J. Netw. Comput. Appl.* **2020**, *172*, 102839. [CrossRef]
84. Hasan, W.K.; Abood, A.M.; Habbal, M. A Review of Blockchain-based on IoT applications (challenges and future research directions). In Proceedings of the 2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA), Sydney, NSW, Australia, 25–27 November 2020.
85. Lin, J.; Long, W.; Zhang, A.; Chai, Y. Using Blockchain and IoT technologies to enhance intellectual property protection. In Proceedings of the 4th International Conference on Crowd Science and Engineering, Jinan, China, 18–21 October 2019.
86. Karthikeyan, P.; Velliangiri, S. Review of Blockchain-based IoT application and its security issues. In Proceedings of the 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, India, 5–6 July 2019.
87. Mezquita, Y.; Casado, R.; Gonzalez-Briones, A.; Prieto, J.; Corchado, J.M. Blockchain technology in IoT systems: Review of the challenges. *Ann. Emerg. Technol. Comput. (AETIC)* **2019**, *3*, 17–24. [CrossRef]
88. Ye, C.; Cao, W.; Chen, S. Security challenges of Blockchain in Internet of things: Systematic literature review. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4177. [CrossRef]
89. Alfrhan, A.; Moulahi, T.; Alabdulatif, A. Comparative study on hash functions for lightweight Blockchain in Internet of Things (IoT). *Blockchain Res. Appl.* **2021**, *2*, 100036. [CrossRef]
90. Alfandi, O.; Khanji, S.; Ahmad, L.; Khattak, A. A survey on boosting IoT security and privacy through Blockchain: Exploration, requirements, and open issues. *Clust. Comput.* **2021**, *24*, 37–55. [CrossRef]
91. Tao, F.; Wang, Y.; Zuo, Y.; Yang, H.; Zhang, M. Internet of Things in product life-cycle energy management. *J. Ind. Inf. Integr.* **2016**, *1*, 26–39. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.