REVIEW ARTICLE

Systematic Literature Review on Blockchain Based IoT Solutions

Muhammad Khurram Umair[1,*], **Muhammad Sohail Khan**[2] **and Muhammad Faisal Abrar**[3]

[1] University of Engineering and Technology Peshawar, Peshawar 25000, Pakistan
[2] Department of Computer Software Engineering, University of Engineering and Technology Mardan, Mardan 23200, Pakistan
[3] College of Computer Science & Engineering, University of Ha'il, Ha'il 2440, Saudi Arabia

Abstract

The growth of the Internet of Things (IoT) has connected a massive number of devices, but its common centralized design creates major security, privacy, and scalability problems that old security methods cannot properly fix. This review explores how Blockchain Technology (BCT) offers a new approach to create trust and strong security for IoT systems without a central authority. Following the PRISMA guidelines, this study analyzes 68 research papers and uses a Chi-square test to statistically confirm the link between IoT problems and the use of blockchain solutions. The results show a strong, statistically proven connection, with a Chi-square value of 34.772 ($p<0.05$) and a Cramer's V of 0.63. Key issues like data integrity, confidentiality, and device identity management are effectively solved by blockchain's features, including smart contracts. The paper also compares leading platforms—IOTA, Ethereum, and Hyperledger—evaluating their pros and cons regarding scalability, speed, and energy use for different IoT applications. This work provides a structured, evidence-based analysis of the Blockchain-IoT landscape, offering critical evaluation that goes beyond simple summaries. It also identifies future research directions, such as combining blockchain with Artificial Intelligence (AI), developing quantum-proof security, and creating universal standards to allow different systems to work together seamlessly.

Keywords: blockchain, IoT, literature review, secure IoT solutions, systematic review.

1 Introduction

The Internet of Things (IoT) has rapidly evolved into a tangible technology, connecting billions of devices and enabling real-time exchange of valuable information. However, amidst this remarkable advancement, IoT devices share common cybersecurity challenges similar to those of other internet systems; these challenges include DDoS attacks, eavesdropping, masquerading, identity theft, data integrity issues, and wormholes. However, unique characteristics that differentiate IoT from other internet systems are their resource constraints (limited resources and processing power) and heterogeneity of devices,

Submitted: 10 July 2025
Accepted: 22 January 2026
Published: 13 February 2026

Vol. 2, **No.** 2, 2026.
10.62762/TACS.2025.327681

***Corresponding author:**
✉ Muhammad Khurram Umair
umair19@hotmail.com

Citation
Umair, M. K., Khan, M. S., & Abrar, M. F. (2026). Systematic Literature Review on Blockchain Based IoT Solutions. *ICCK Transactions on Advanced Computing and Systems*, 2(2), 116–136.

with diverse devices ranging from simple sensors to complex smart devices. These differences pose challenges for applying traditional cybersecurity measures compared to their application on more powerful and complex internet systems (i.e., servers, computers, and network machines) [1]. Potential challenges related to privacy and security are of significant concern in IoT implementations [2]. To address such issues in IoT implementation, the integration of Blockchain Technology (BCT) has emerged as a promising solution. BCT offers several advantages in addressing IoT's unique cybersecurity challenges, including decentralization to mitigate DDoS attacks, and immutability and transparency for addressing eavesdropping, masquerading, fake data, and identity theft issues. Additionally, BCT offers lightweight consensus mechanisms critical for resource-constrained IoT devices, thus enabling IoT devices to securely participate in a network even with limited processing power [3].

This paper seeks to provide a focused understanding of how BCT can enhance IoT implementations and address areas such as security breaches and unauthorized data access. Key challenges related to IoT are as follows:

- **Data Privacy and Confidentiality:** Ensuring that personal and sensitive data transmitted through IoT networks remains protected from unauthorized access.
- **Data Integrity:** Preventing data tampering during transmission among different IoT devices and maintaining the accuracy and authenticity of the data.
- **Authentication and Authorization:** Securely verifying the identity of IoT devices and ensuring that only authorized devices can access critical system functions.
- **Scalability and Interoperability:** Ensuring that IoT systems can scale effectively without compromising security, allowing different IoT devices to operate together securely.

By nature, IoT is inherently distributed due to interconnected heterogeneous devices that operate autonomously and communicate by exchanging real-time data. These devices can be geographically distributed and might range from simple devices to complex systems, thus these diverse devices create significant challenges in terms of data management, security, and interoperability. BCT addresses these challenges by utilizing a distributed ledger that ensures data is securely replicated across several nodes in a network without the need for a central server. It is important to further differentiate between decentralized and distributed architectures: decentralization refers to the absence of a central authority or single point of control, where data processing is spread across multiple nodes. This distributed, secure data storage facilitates risk mitigation in IoT systems through the avoidance of potential single points of failure; therefore, it makes IoT ecosystems resilient to Distributed Denial of Service (DDoS) attacks. The structure of the paper is as follows: Section 2 covers a brief background of the issues related to IoT implementation and the potential of Blockchain technology to mitigate these challenges. Section 3 outlines the research methodology, details about literature selection criteria, and the analytical approach for conducting the Chi-square test. Section 4 presents key insights of the study, implications for future research, and practical applications. Moving forward, Section 5 delves into the specific security issues encountered in IoT and presents an overview of how Blockchain integration can address these challenges. Section 6 discusses the results related to the association between IoT issues and the proposed solution of Blockchain. In Section 7, different Blockchain-based platforms are discussed, including IOTA, Ethereum, and cloud-based Blockchain as a Service. Section 8 proposes future work directions with the integration of AI with Blockchain and IoT, and lastly, Section 9 provides a conclusion of the study conducted and the potential of Blockchain for addressing IoT's inherent issues. By exploring the existing literature, we identify key insights related to the implementation and effectiveness of BCT for addressing issues such as single points of failure, privacy, and security. These insights not only shed light on the current state of research but also serve as a foundation for future studies and practical applications aimed at strengthening the framework of IoT.

2 Background

The Internet of Things (IoT) revolutionizes the way smart objects connect and collaborate, enabling efficient data collection and informed decision-making. This transformative technology has the potential to address numerous everyday challenges and enhance the quality of human life. However, the centralized nature of traditional IoT architectures poses scalability issues, including concerns related to data privacy, single-point failures, and data integrity. These

challenges impede the future development and expansion of IoT. To overcome these limitations, the integration of Blockchain technology presents a decentralized and distributed architecture, offering enhanced efficiency for IoT systems. By leveraging the power of Blockchain, IoT implementations can achieve improved security and privacy through the utilization of cryptographic methods to safeguard sensitive data from potential threats. This integration not only addresses the existing challenges but also paves the way for a more robust and resilient IoT ecosystem. The Internet of Things (IoT), which was first envisioned by Kevin Ashton in 1998 [4], represents a recent revolution in communication between devices. Ensuring security and privacy in IoT implementations is quite challenging to accomplish [5], as millions of sensors with heterogeneous architectures are interconnected for real-time data exchange [6, 7]. The centralized architecture of IoT devices has many advantages for interconnecting multiple devices that can be managed with a single server [8]. Although many IoT platforms are designed with centralized control, the inherent distribution of devices and data makes IoT systems more susceptible to issues that can be effectively addressed by distributed ledger technologies like Blockchain [9]. The diversity of IoT devices, ranging from low-power sensors to more complex devices, necessitates a security and data management framework that can handle the complexity of real-time, distributed data exchange. Blockchain provides a framework where data is not stored in a single location but is instead replicated across multiple distributed nodes, offering enhanced security, transparency, and scalability [10]. This research investigates the critical issues of IoT implementation specifically related to cybersecurity. While privacy, security, and confidentiality are universal concerns across numerous platforms, the Internet of Things (IoT) encounters unique challenges that are not adequately addressed by traditional security mechanisms employed in other platforms. For instance, IoT devices are typically resource-constrained (e.g., limited processing power and storage), rendering it challenging to apply conventional security solutions that rely on substantial computational resources or centralized management. Furthermore, IoT systems are often highly heterogeneous, comprising a diverse range of devices with varying capabilities, making uniform security protocols difficult to implement. Consequently, IoT necessitates specific solutions tailored to its unique nature, which is why Blockchain Technology (BCT) presents a promising approach, offering decentralized, lightweight, and scalable security.

3 Literature review

The advent of the Internet has revolutionized various aspects of human life, transforming communication, interaction, and even transportation. In the present era, home appliances and devices are interconnected, thus enabling remote control via internet-based applications. The concept of the "Internet of Things (IoT)" revolves around the idea of creating a network where smart devices can autonomously communicate with each other using the internet architecture. The primary goal of IoT is to enhance the convenience of everyday life through automation [11]. Figure 1 provides a basic overview of the IoT ecosystem, illustrating the interconnected nature of various devices and their communication pathways.

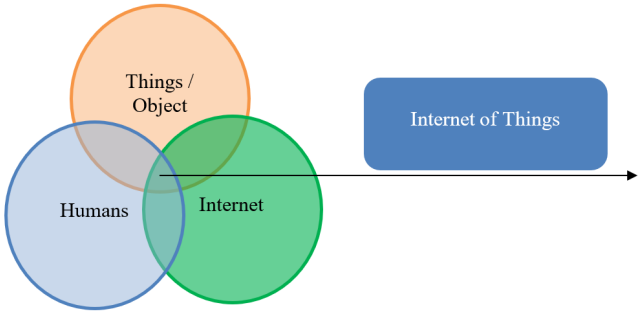

Figure 1. IoT Illustration.

The pervasive influence of the Internet in daily lives is undeniable, as it continues to extend its reach to every corner of the globe. However, this technological revolution is still evolving and has yet to fully realize its potential. With the advancement of connectivity, an increasing number of appliances and devices are now able to connect to the web, ushering us into the era of the "Internet of Things" (IoT). The IoT encompasses a vast network where objects and devices, regardless of their nature, can possess networking and computational capabilities. This connectivity enables objects to be monitored and modified remotely, leveraging query and modification capabilities. Essentially, the IoT creates an interconnected environment where the majority of devices are seamlessly integrated into a single network. Through this integration, complex challenges that demand ingenuity and innovative thinking can be tackled [11].

3.1 Architecture of IoT

The architecture of the Internet of Things (IoT) lacks a universally accepted standard, as highlighted in [12]. Researchers have proposed various architectural models, including the 3-tier and 5-tier architectures, which emerged during the early stages of this field of study [13]. The 3-tier architecture consists of three layers: perception, logistic/network, and application. However, the literature suggests more layered designs to capture the complexity of IoT systems, such as 4-tier and 5-tier architectures. One such example is the five-tier architecture, which incorporates additional layers of business and processing as additional layers in the same 3-tier architecture. The five layers in this architecture are perception, logistics, processing, applications, and business. The perception, logistic/network, and application layers perform similar functionality in the five-tier architecture as in the three-tier architecture. Broadly, the overall functioning of each architectural layer covered in both 3-tier and 5-tier architectures is described in [14], and the responsibility of each layer is summarized below:

- Perception layer: Responsible for data collection from sensors.
- Logistics layer: Also called the network layer, it manages the routing of collected data.
- Processing layer: Responsible for data filtering, aggregation, normalization, and analysis.
- Application layer: This layer may include various software applications.
- Business layer: It involves integrating IoT data with business processes and systems.

3.2 Security and Privacy in IoT

As far as IoT implementations are concerned, the privacy of data cannot be left unchecked. Preserving data secrecy and identity during transmission in heterogeneous network is a great challenge to accomplish. In this regard, different counter-measures have been suggested in existing literature as discussed in [15]. To understand the key challenges faced by IoT implementation regarding security and privacy of the data, a few common issues are listed in Table 1.

3.3 Blockchain

A Blockchain refers to a decentralized database that computer network nodes share. By digitally recording data, a Blockchain acts as a database. Blockchain plays an essential role in cryptocurrency systems such as Bitcoin in preserving a secure and distributed record of transactions [16, 17]. The Blockchain develops trust without any dependency on third party architecture and also maintains the security and integrity of a data record. As per the details available in literature, it is evident that Blockchain data structure is completely different from the regular database structure. In a Blockchain, data is grouped into unit's series of blocks, which each comprises a set of data. When a block utilizes all of its allocated storage, it is closed and connected to another block before it, thus creating a chain of data that's why known as Blockchain [18]. Once the chain is filled, a new block is created from all information added after the just-added block and added to the chain. A Blockchain is logically described as the collection of blocks that are connected by a network and each block carry a specific piece of information (peer-to-peer database). In other words, Blockchain refers to a network of connected computers as opposed to a single server, indicating that the network as a whole is decentralized. A Blockchain architecture enables the dissemination of digital information as opposed to its duplication using distributed ledgers thus offers data protection, transparency, and trust [19].

Blockchain Technology (BCT) operates as a distributed ledger, maintained across a peer-to-peer network. This distributed nature allows Blockchain to achieve decentralization, thus, eliminating the need for central controlling authorities to verify transactions. Transactions are validated by each node using consensus algorithms such as Proof-of-Work (PoW), Proof-of-Stake (PoS) and others, by agreeing on the validity of transactions before the transaction is added to BCT network. This consensus mechanism also ensures that the network is coherent and trustworthy, providing an immutable record of transactions. Each block in the Blockchain are mathematically linked with another block using a cryptographic hash function. Each block contains a hash of the previous block, creating a chain of blocks making BCT a tamper-proof technology. Block's ID is generated by hashing the contents of the block along with the ID (hash) of the previous block. To ensure this process is secure, a nonce (a random number used once) is added during the consensus process to create a unique hash for each block. This nonce guarantees that the cryptographic hash is unique for each block, and modifying any block would require recalculating the hash of all subsequent blocks, which is computationally infeasible.

This mathematical linkage ensures that once data

Table 1. Challenges faced by IoT.

Challenges	Description
Single Point of Failure	In basic IoT framework utilizes centralized architecture where single server to manages the various devices if the server goes down no device will connect or work in the network [10].
Security	In centralized IoT framework data storage and processing take place at single point. So, IoT based devices and applications are more vulnerable to threats [8].
Privacy	Different type of data collected from IoT devices and this data store at one location will violate data privacy easily [4, 6].
Inflexibility	The IoT centralization concept will make it inflexible because large amount of data create load on server and results to delay in the linking process [12].
Cost	In IoT, central server performs all processing and communicating devices. It also needs huge storage to store large amount of data coming from various IoT devices all capabilities will increase the cost [17].
Scalability	The managing of all nodes by central server can scale well in small network. However, if the IoT devices increases it will create scalability issues in IoT network [13].
Access and diversity	Among the most important challenge of centralized system to provide access to all users for their diverse needs. A large IoT network has serious issue of access to all users [14].

is added in the Blockchain, it cannot be altered without the consensus of the network. If a single block is altered, the hash for that block changes, and subsequently, all subsequent block hashes must be recalculated to maintain the integrity of the Blockchain. This mathematical linkage guarantees the immutability of the data, thus making it tamper-proof and provide an additional layer of trust in the Blockchain's operations.The use of cryptographic tools, including symmetric and asymmetric encryption, enhances the security of data within the Blockchain. Asymmetric encryption is used for public-key cryptography, where each participant has a public and private key, ensuring that data can only be accessed by authorized users, while symmetric encryption ensures the confidentiality and integrity of data shared between participants.

In this context, the nonce used in the Proof-of-Work consensus algorithm is essential for the security of the Blockchain. It ensures that the hash of a block is not predictable, and the computational effort required to find the correct nonce makes it impractical for malicious actors to alter the Blockchain. This method of mathematical linking, combined with cryptographic validation, ensures coherence, logic, and trust across the Blockchain network.

A large volume of academic literature supports such claims and further delves into the cryptographic mechanisms used in the design of Blockchain. For instance, Leva et al. [20] describe the nonce as playing a significant role in the Proof-of-Work process by requiring computational effort in finding the correct hash, ensuring the integrity of the Blockchain. Miraz et al. [21] also draw attention to how the distributed consensus implemented in Blockchain makes the information or data immutable and tamper-proof by using the cryptographic hash functions in combination with asymmetric encryption. These form the essence of why Blockchain is a suitable solution for ensuring data integrity in decentralized systems like IoT.

3.4 Blockchain Components

Core components of the Blockchain are blocks, ledgers, hashes, transactions, miners and consensus mechanisms. A brief definition of these functional components are as follows:

- **Block:** Block is the primary component; each block comprises a set of transaction. The blocks are chained together with a unique hash value of the previous and current block creating a tamper evident record of all transactions that have taken place on the Blockchain network. The block also contains the nonce, a unique random number used in the Proof of work (PoW) consensus algorithm, ensuring that the block is cryptographically linked to the previous one. This makes it computationally infeasible to change any block without recalculating all subsequent block, ensuring immutability.
- **Ledger:** The ledger is a data structure which stores information of all transaction on the Blockchain network and is different from traditional databases, as the ledger is decentralized and maintained by all participating nodes in the network, thus ensuring no single point failure. Every participants of the network holds a copy of ledger, thus ensuring transparency and resilience against tampering.

- **Hash:** The hash function is a mathematical problem that should to be solved by miners and the resulting hash value is unique to the content of the block and serves as a digital fingerprint to validate the integrity of the block. Hash functions used in Blockchain, such as SHA-256, are collision-free which means, no two different inputs will produce the same hash value [22]. This ensures that any modification to the content of a block will result in a completely different hash, making it easy to detect tampering and this process is critical to immutability and security of BCT.

- **Transaction:** A transaction is the smallest operation, representing a transfer of value or data between two parties. Transactions are grouped together in blocks and must be validated by miners before they can be added to Blockchain. The size of a transaction is important for miners to estimate the compute resources required.

- **Miners:** Miners are nodes (computers/agents with specialized hardware and software) that compete to solve hashes to explore a new block. Discovered new block is added to the network and broadcasting it to all nodes for verification and then each node combines a set of transactions into a block and operates to discover the block's proof-of-work [12].

- **Consensus Mechanisms:** Consensus mechanisms are the protocols that Blockchain networks use to agree on the validity of transactions. Proof-of-Work (PoW), for example, is used in Bitcoin, requires miners to perform computational work to solve puzzles and validate new blocks. In contrast, Proof-of-Stake (PoS), selects validators based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. Other mechanisms like PBFT, Practical Byzantine Fault Tolerance, are also used in different Blockchain implementations, such as Hyperledger. These consensus algorithms ensure that all nodes in the network agree on the state of the Blockchain, even without a central authority, thus providing coherence, trust, and resilience.

3.5 Existing Body of Knowledge (BoK) on IoT with Blockchain

The most intriguing area of this research is Blockchain integration with IoT. The challenges identified in centralized architecture IoT implementations are addressed by the decentralized architecture of Blockchain. IoT vulnerabilities were reviewed in [23]. IoT security related challenges are listed and discussed vis-à-vis their potential solutions using Blockchain technology are discussed in [24]. Furthermore, a discussion on how Blockchain architecture addresses security concerns in both conventional IoT and commercial IoT implementations is also covered in [25]. Furthermore, Alkurdi et al. [24] describes a lightweight IoT architecture that is built on the Blockchain technology. Further studies presented in [26, 27] and [28] enlightens the efficacy of Blockchain technology implementation to address data security, integrity and privacy related inherent issues of IoT centralized architecture. In order to guarantee the integrity of sensing data, Hang and Kim [27] presented an integrated IoT platform employing Blockchain technology. Their suggested platform made it possible for the users to operate and monitor devices in real time. The findings presented in the paper discusses that suggested platform works well for resource-constrained IoT devices. Additionally, Polyzos et al. [29] explain the advantages of using technology to examine the security requirements of IoT devices and how integrating IoT with Blockchain may assist address these security challenges. Mahmood et al. [30] examined IoT security challenges before proposing Blockchain as a viable solution. A smart service agreement approach was recommended in [31] to solve security and privacy problems in the IoT system and enable secure communication between IoT devices. The proposed system is based on Blockchain technology, enabling decentralized network access, authentication, and communication. Tandon [32] gave an overview of Blockchain technology and how it is the best way to manage the security and privacy issues that the IoT system presents. The report also covered the advantages and difficulties of combining Blockchain and IoT. The requirements for developing an identity management system for the Internet of Things were reviewed and suggestion on combining Blockchain technology with the IoT for a reliable identity management system to offer improved performance and trust is discussed by Zhu et al. [33]. An Ethereum based framework is suggested by Kadam and John [34] for low-power IoT devices based on the Ethereum Blockchain to address the inherent problem in IoT devices while authenticating transactions, and offering security. The centralized architecture of IoT would not be effective for such large-scale IoT network thus decentralizing using Blockchain is suggested to overcome single point

failure issues related to centralized architecture of IoT [35]. The centralized server approach is the foundation for the vast majority of IoT systems now in use. Devices in IoT systems collect data from targeted objects and enable data transfer to a centralized computer through a wired network to the internet. According to the requirements and ease of the users, analytics were performed from the centralized server. In a similar vein, if a large-scale IoT system intends to do analysis, present infrastructure processing capabilities may not be sufficient [36].

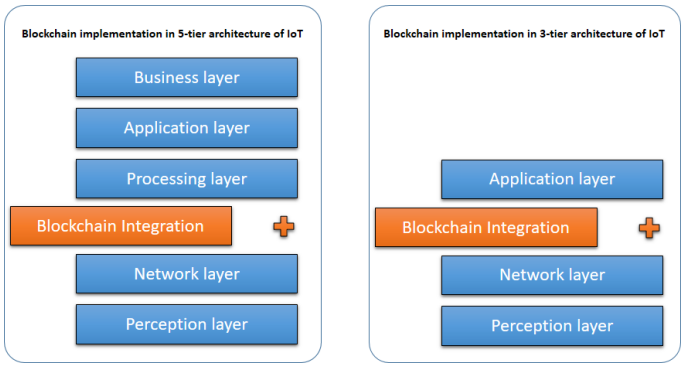

Figure 2. Implementation of blockchain in IoT architecture.

3.6 Blockchain in IoT Use Cases

Apart from discussing the implementation of Blockchain in IoT architecture, literature also presents the efficacy of Blockchain in different application of IoT in everyday life. For example, in Health care, Badr et al. [37] discussed the implementation of Blockchain for securing patient data. Similarly, Patil et al. [38] suggested implementation of Blockchain for interconnected IoT devices for smart greenhouse farms with improved security and privacy in agriculture. Similarly, Kamilaris et al. [39] also suggested the benefits of Blockchain in agriculture and food chain. Moreover, Rajeb et al. [40] provided a review of Blockchain based supply chain management system with integrated IoT devices. In E-business, Blockchain ensures added security [41]. In industrial IoT (IIoT) the challenges are overcome with distributed ledger technology with IoT and 5G technology as discussed in [42].

3.7 Implementing Blockchain in IoT Architecture

After reviewing the existing BoK, it is evident that most of the researcher agreed that Blockchain is potential candidate to resolve the inherent issues of IoT centralized architecture. Integrating Blockchain in IoT architecture can be achieved in numerous ways. However, one most commonly suggested method of integration is in a layered architecture. As discussed earlier in Section 3.1, IoT basic architecture comprises of three-layered architecture and additional layers (four, five and six) can be added as per the business / industrial requirements. Integrating Blockchain in existing architecture can be achieved by integration Blockchain layer as a separate additional layer between network and application layers of IoT architecture. Conceptual demonstration of the same is depicted in Figure 2 for both three-layered as well as five-layered architecture of IoT.

The first layer, perception layer, of the IoT architecture is where the sensors, actuators exists to sense and gather the data of the surrounding environment. Key responsibility of this layer is sense the environment and generate data to upper layers, i.e. as an smart health gadget the sensors will sense the health related data e.g steps taken, sleep monitoring, activity performed etc. and after gathering the data this layer send the data to upper layer, network layer. The network layer is responsible to provide connectivity of the IoT sensors / devices to external world and performs the network and routing management of all IoT objects connected. This layer can be part of the IoT device or might be an external device is used to connect a sensor to the network. In both cases, the network layer is only responsible for network connectivity, enabling communication and security management. Conceptually, the best suited place for integrating Blockchain with IoT in layered architecture is after network layer. This new Blockchain layer involves all modules that enable various features of the Blockchain technology, such as distributed ledgers, smart contracts, consensus management and identity management, to be integrated in IoT architecture [43].

To provide a comprehensive overview of the Blockchain-IoT integration landscape explored in this systematic literature review, Figure 3 presents a detailed taxonomy that synthesizes the key findings from our analysis of 86 research publications. This taxonomy illustrates the hierarchical relationships between IoT challenges, blockchain solutions, implementation platforms, application domains, and future research directions, while also demonstrating the statistically validated associations (χ^2=34.772, $p<0.05$) between identified challenges and proposed blockchain-based solutions.

4 Research Methodology

After presenting the detailed literature review, guidelines proposed by Preferred Reporting

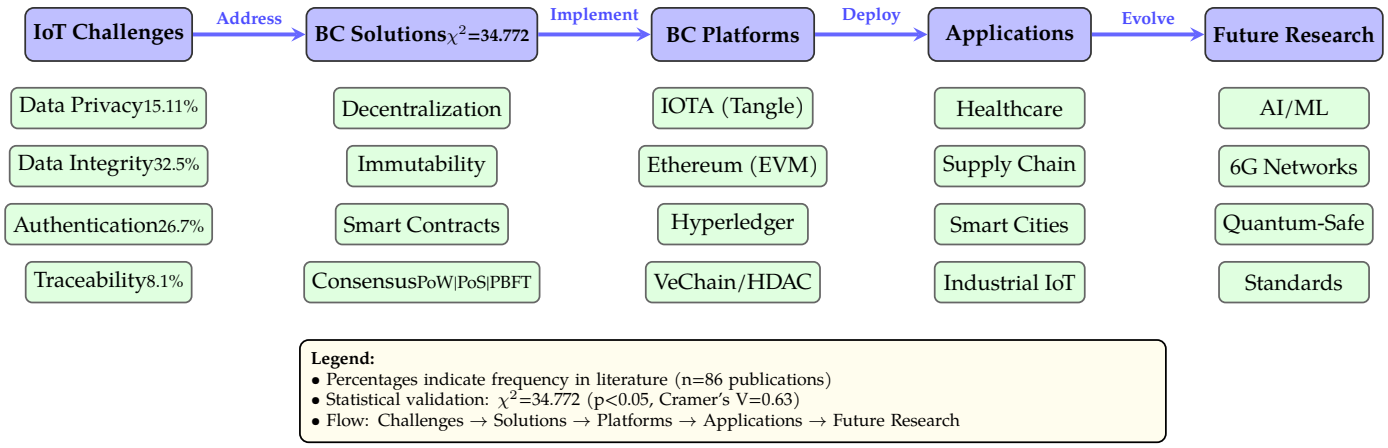

Figure 3. Blockchain-IoT Integration Taxonomy: A systematic framework showing the progression from IoT security challenges through blockchain solutions, implementation platforms, real-world applications, to future research directions. Based on analysis of 86 publications with statistical validation (χ^2=34.772, p<0.05, Cramer's V=0.63).

Items for Systematic Reviews and Meta-Analyses (PRISMA) research methodology (SLR) is selected to documenting the research. Aim of the research conducted is to identify the key issues faced by IoT and to find out how Blockchain is potential candidate in resolving the key issues such as security and privacy of data in IoT implementation. Subsequently, a detailed study of existing Body of Knowledge (BoK) is consulted to validate the association of Blockchain technology in resolving the key issues associated with IoT implementations.

4.1 Inclusion and Exclusion Criteria

Inclusion / Exclusion criteria is made for the selection and shortlisting of the literature:

- Published in English.
- Peer-reviewed.
- Focused on the use of Blockchain-based solutions in IoT.
- Reported security and privacy-related issues in IoT.
- Proposed a Blockchain-based solution to address IoT inherent issues.

Studies that did not meet the above mentioned inclusion criteria or duplicates were excluded. Studies focused on Blockchain-based solutions in domains other than IoT, or that did not associate with key issues pertaining to IoT implementation were also excluded. Data from the included studies was extracted using a predefined data extraction form which includes information related to study characteristics (e.g., authors, year, country); study design (e.g., case study, experiment, survey); Blockchain solution characteristics (e.g., type, implementation, performance); and identifying issues related to IoT (e.g., data integrity, access control, confidentiality). The extracted data were synthesized and analyzed qualitatively.

4.2 Research Questions

As an initial step, is to define the Research Questions (RQs). The RQs defined for this SLR are listed in Table 2.

4.3 Hypothesis – Required for RQ1 and RQ2

In order to address the RQ1 and RQ2, the Chi-square analysis was used to test the relationship between the use of Blockchain-based solutions and security and privacy-related issues in IoT. The null hypothesis is stated as "there is no significant difference in security and privacy-related issues between studies that propose or evaluate a Blockchain-based solution". The alternative hypothesis is stated as "there is a significant difference in security and privacy-related issues between studies that propose or evaluate a Blockchain-based solution" as shown in Table 3.

4.4 Search String

Articles were searched from electronic databases such as IEEE Xplore, SpringerLink, Google Scholar, Science Direct, and ACM are among the electronic databases and also relevant conference proceedings and journals where searches are conducted. After applying the inclusion and exclusion criteria, as mentioned in section 4.1 above, a total of 30 articles were identified for analysis. The articles included in our analysis were published between 2015 and 2022 and covered a wide

Table 2. Research questions used in research.

No.	Research questions
RQ1	What are the security and privacy related issues in IoT?
RQ2	How Blockchain based solution overcome these issues in literature review?
RQ3	What are the available Blockchain platforms for IoT applications?

Table 3. Research hypothesis formulated for the article.

Hypothesis	Details
Null (H0)	There is no significant relationship between Blockchain-based solutions and the security and privacy related issues addressed in IoT.
Alternate (H1)	There is significant relationship between Blockchain-based solutions and the security and privacy related issues addressed in IoT.

range of topics related to security and privacy issues in IoT and the use of Blockchain-based solutions. . The Internet of Things, IoT, Blockchain, B-IoT, IoT security and Challenges are thus defined as a set of terms relevant to this study subject. Finally, search strings were created to collect the published publications relevant to the research subject. Search strings are mentioned in Table 4.

4.5 Study Selection

The study selection procedure entails doing a tollgate approach search in digital libraries using the search strings as a guide. A selection of papers is shown in Figures 4 and 5. The initial selection process involved

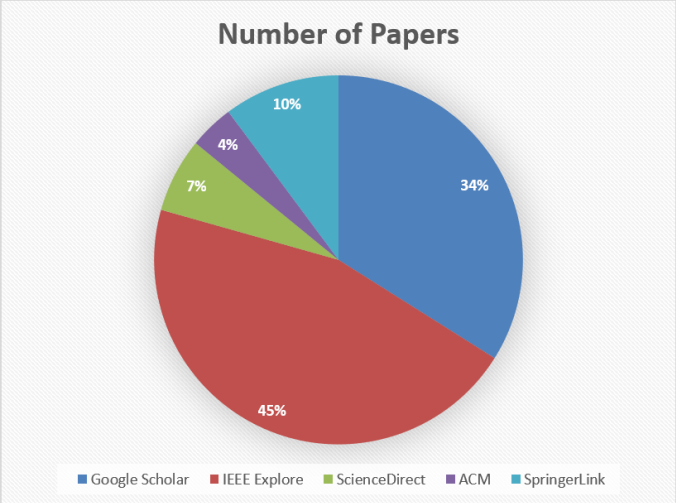

Figure 4. Selected Literature distribution.

a search technique on the selected digital libraries, resulting in a pool of 396 publications. This selection was based on keywords, titles, duplicate elimination, and thorough examination of abstracts and complete papers. After a rigorous selection process, a total of 86 publications were shortlisted for this research. Details of selected 86 research publications are mentioned in Appendix A. Summary of the overall paper selection process, outlining steps taken till final shortlisting of the publications is mentioned in Table 5

5 Analysis & Discussion (RQ1 and RQ2)

To respond to RQ1, the SLR identified challenges/critical issues, which are summarized in Table 6 and discussed in the following sub-sections. Major disparity in the security difficulties faced by IoT devices is observed. A challenge percentage range of 40% to 50% is settled and in the highlighted problems, "Identity Management & Authentication, Confidentiality, Data Integrity & Availability, Anonymity and Data Privacy", are the identified challenges.

5.1 Challenges Based on Digital Libraries Comparison

The examination of the highlighted difficulties based on digital libraries is shown in Table 7. The search libraries are IEEE Xplore, Google Scholar, Science Direct, ACM, and Springer Link.

5.2 Comparison of challenges based on Timeframe

The timeframe based comparison period is conducted by separating the overall selection into two timeframes. Timeframe 1 covers the years 2005 to 2015 while Timeframe 2 covers the years 2016 to 2021. Table 8 shows a timeframe-based examination of the highlighted difficulties:

5.3 Proposed Solutions

In order to answer RQ2, the solutions suggested for the inherent issues faced by IoT and highlighted in research publications are covered in the section below, which discusses the implications of integrating IoT with Blockchain. Even though the integration of

Table 4. Search string formulated for different sources to filter research articles based on relevance.

Sources	Search String
Google Scholar	(IOT security) AND (Blockchain IOT) AND (Blockchain IoT overcome security issues)
IEEE Explore	(Blockchain & IOT security) AND (IoT OR "Internet of Things") AND Challenges
ScienceDirect	(Internet of Things security solutions) AND (Blockchain IoT) AND (Blockchain Security)
ACM	(Security challenges in IoT) AND (Blockchain security)
SpringerLink	(IoT security challenges) AND ("Blockchain IoT) AND (b-IoT security)

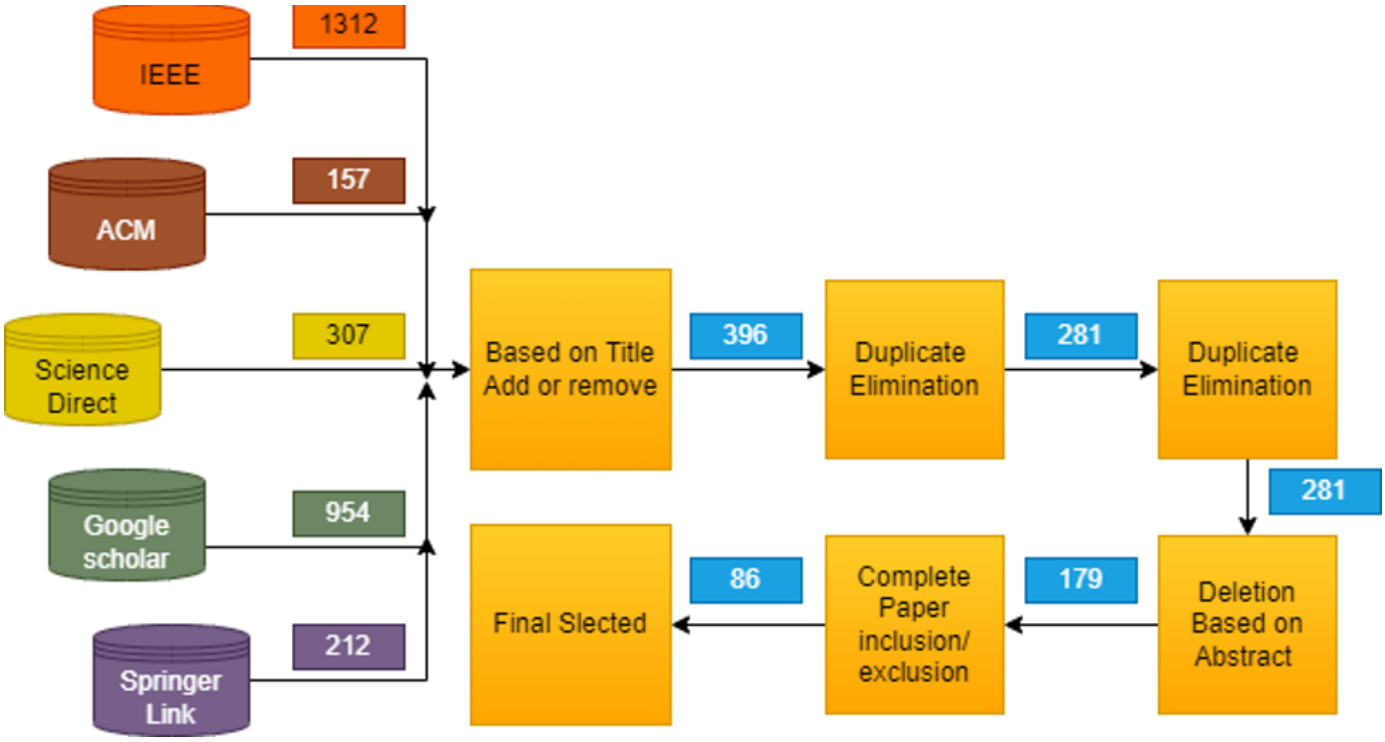

Figure 5. Literature selection process with source.

Table 5. Filters applied on selection of research articles to find out the relevant research articles from each source.

No	Selection Criteria	Science Direct	ACM	Springer Link	Google scholar	IEEE Xplore	Total
1	Keywords	307	157	212	954	1312	2942
2	Titles	29	18	41	132	176	396
3	Duplicate Elimination	19	16	32	91	123	281
4	Abstract	30	13	18	51	67	179
5	Complete Papers	14	5	7	27	33	86

IoT with Blockchain was just recently accomplished, various IoT applications have already been presented to benefit from the features of Blockchain, such as end-to-end traceability, confidentiality and information security, identity authentication, availability, data integrity, and privacy. Table 9 presents the solutions proposed in the selected literature.

Blockchain offers better security implementations for IoT applications with features such as decentralized architecture with no single point of failure, distributed systems where resources are shared, and data transfers that cannot be altered by a single node. This research article focuses on increasing the security of IoT by keeping data private and anonymous, using verification and identity authentication, and using Blockchain technology to ensure data is valid, available, and confidential. It also suggests solutions on how Blockchain and IoT can achieve end-to-end traceability.

Table 6. Challenges identified through Systematic Literature Review (SLR).

S. No	Challenges	Frequency	Percentage	Papers ID
1	Blockchain Integration Possibilities	6	6.97%	P1, P4, P7, P33, P38, P44
2	Information Processing and Sourcing Blockchain-IoT	9	10.4%	P5, P9, P32, P37, P43, P47, P57, P59, P60
3	End to End Traceability	7	8.1%	P2, P30, P31, P36, P41, P42, P48
4	Anonymity and Data Privacy	13	15.11%	P10, P13, P29, P34, P35, P61, P69, P73, P74, P75, P80, P81, P84
5	Identity Management / Authentication	23	26.7%	P6, P15, P17, P18, P27, P39, P40, P49, P52, P53, P54, P56, P64, P66, P67, P76, P77, P78, P79, P82, P83, P85, P86
6	Confidentiality, Data Integrity, and Availability (CIA)	28	32.5%	P2, P3, P8, P11, P12, P14, P16, P19, P20, P21, P22, P23, P24, P25, P26, P28, P45, P46, P50, P51, P58, P62, P63, P65, P68, P70, P71, P72

Table 7. Paper selection from digital libraries.

Source	Google Scholar (n=27)		IEEE Xplore (n=33)		ACM (n=5)		Springer Link (n=7)		Science Direct (n=14)	
Challenges	**f**	**%**	**F**	**%**	**F**	**%**	**F**	**%**	**F**	**%**
Information Processing and Sourcing Blockchain-IoT	3	11	3	9	1	20	0	0	2	14
End to End Traceability	2	7	2	6	0	0	2	28	1	7
Anonymity and Data Privacy	6	22	4	12	1	20	0	0	2	14
Identity Management / Authentication	4	15	13	39	1	20	2	28	3	21
Confidentiality, Data Integrity and Availability (CIA)	10	37	8	24	2	40	3	43	5	36

Table 8. Summary of timeframe-based examination.

Challenges	Timeframe-I (2005–2015) n = 39		Timeframe-II (2016–2021) n = 47	
	f	**%**	**f**	**%**
Information Processing and Sourcing Blockchain-IoT	3	7	6	13
End to End Traceability	4	10	9	19
Anonymity and Data Privacy	7	18	6	13
Identity Management / Authentication	8	20	15	32
Confidentiality, Data Integrity, and Availability (CIA)	11	28	17	36

5.4 Statistical Analysis of results

Challenges in this SLR were identified using the Chi-Square test method as per the data presented in Table 10 above. To perform the Chi-square test for independence, the data is organized in a contingency table. Six challenges are categorized into two broader categories: Blockchain-based solutions and non-Blockchain-based solutions.

Based on the contingency table, the test for calculating expected frequencies, degrees of freedom, and chi-square values can be performed to determine whether there is a significant relationship between Blockchain-based solutions and the issues highlighted in different publications. A significance level of 0.05 is set to calculate the expected frequency, degrees of freedom, and Chi-square values as follows: **Expected Frequency Calculation:**

$$\text{Expected Frequency} = \frac{\text{Row Total} \times \text{Column Total}}{\text{Grand Total}}$$

Table 9. Summary of solutions for identified challenges.

Challenge Addressed	Proposed Solutions			
	Ref	Year	Approach	Solution
System for Information Processing and Sourcing Blockchain-IoT	[44]	2017	Framework	Provide solutions of data loss in IOT with the use of Block chain
	[45]	2010	Framework	
	[46]	2017	Framework	Malicious IoT devices tracked via Blockchain
	[48]	2020	Platform	
End to End Traceability	[44]	2016	Framework	IBM's Blockchain-based supply chain platform
	[51]	2018	Framework	Blockchain based product traceability
	[52]	2019	Framework	Malicious IoT devices tracked via Blockchain
	[54]	2009	Platform	Smart contracts tracks agricultural supply chains
	[65]	2016	Framework	OriginTrail provides data confidentiality
Anonymity and Data Privacy	[53]	2018	Approach	Data aggregating and confidentiality technique using Blockchain
	[66]	2018	Platform	Ethereum based platform for data privacy
	[67]	2018	Framework	Security and privacy in decentralized energy trading through multi-signatures, Blockchain
Identity Management /Authentication	[55]	2018	Approach	IoT access control and authentication management via Blockchain
	[56]	2018	Approach	Out-of-band authentication using Blockchain
	[57]	2019	Framework	Filament to enable independent, decentralized connectivity with digital devices, including smart home appliances
	[58, 59]	2014	Framework	Name Coin is to develop a peer-to-peer DNS network based on Bitcoin
Confidentiality, Data Integrity and Availability (CIA)	[61]	2016	Platform	Thingsjs, A JavaScript-based middleware platform bypasses system-specific complexities
	[62]	2017	Architecture	This architecture, supports intelligent decision-making and automates service creation.
	[63]	2014	Platform	IoTOne, Software platform to supports heterogeneous IoT devices
	[61]	2017	Middleware	Cuttlefish, for heterogeneous devices utilization
	[50]	2020	Mechanism	eWoT, provides SPARQL query-based mechanism for transparent discovery and access.

Table 10. Contingency table.

Challenges	Blockchain based solutions	Non Blockchain based solutions	Total
Blockchain Integration Possibilities	6	80	86
Information Processing and Sourcing Blockchain-IoT	9	77	86
End to End Traceability	7	79	86
Anonymity and Data Privacy	13	73	86
Identity Management / Authentication	23	63	86
Confidentiality, Data Integrity, and Availability (CIA)	28	58	86
Total	86	430	516

For example, the expected frequency for Blockchain solutions is:

$$E_{\text{Blockchain}} = \frac{86 \times 86}{516} = 14.333$$

And for Non-Blockchain solutions:

$$E_{\text{Non-Blockchain}} = \frac{86 \times 430}{516} = 71.666$$

Degrees of Freedom (df):

$$df = (r-1)(c-1)$$

where r is the number of rows and c is the number of columns. So:

$$df = (6-1)(2-1) = 5 \times 1 = 5$$

Chi square value for each cell as shown in Table 11. Chi Square distribution table with 5 degrees of freedom and a significance level of 0.05 to find the critical value of Chi Square. The critical value, p, for a Chi Square test with 5 degrees of freedom and a significance level of 0.05 is p = 11.07. The Cramer's V statistic, which is a measure of the strength of association between two categorical variables can be calculated using the formula below:

$$V = \sqrt{\frac{X^2}{N \cdot (\min(r-1,\ c-1))}}$$

where N is the total number of observations, r is the number of rows, and c is the number of columns and X2 is Chi Square calculation. Using the values from our contingency table and Chi Square calculation, we can calculate Cramer's V as 0.63. Cramer's V ranges from 0 to 1, with larger values indicating a stronger association between the two variables. In our case, the value of 0.63 indicates a moderate to strong association between the use of Blockchain-based solutions and the security and privacy-related issues in IoT.

6 Results (RQ1 and RQ2)

Chi-square test for independence is conducted to investigate the relationship between Blockchain-based solutions and the security and privacy related issues addressed in IoT. The calculated Chi-square value was 34.772 with 5 degrees of freedom, which was greater than the critical value of 11.07 at a significance level of 0.05. Therefore, the null hypothesis is rejected thus, there is a significant association between Blockchain-based solutions and the security and privacy related issues addressed in IoT. In addition, the effect size of the relationship between Blockchain-based solutions and the security and privacy related issues addressed in IoT using Cramer's V coefficient is calculated. We obtained a value of 0.63 which also supports association between the use of Blockchain based solutions and security and privacy related issues in IoT implementation.

7 Blockchain Platforms for IoT (RQ3)

The Blockchain concept was first conceptualized by Nick Szabo in 2005 and later introduced as a solution for secure financial transactions of Bitcoin by Satoshi Nakamoto in 2009. However, the application of Blockchain technology has not remained limited to cryptocurrency, and this technology presents multipurpose variations in different fields of life, such as IoT. Combining Blockchain with IoT can provide countless benefits for various IoT applications [44]. However, implementing Blockchain in existing use cases of IoT, such as healthcare, smart homes, smart cities, smart transportation, and others, is quite difficult and challenging. This implementation requires careful selection of a Blockchain platform to be implemented with the IoT system. Different implementations of Blockchain with IoT exist; the most common implementations include IOTA, VeChain, WaltonChain, Ethereum, Hyperledger, and HDAC. These implementations offer key abilities for hashing different transactions, block connectivity, enhanced security and privacy, consensus management, and smart contracts [28].

7.1 IOTA

IOTA is an open-source platform based on distributed ledger technology. The data structure used to handle transactions is acyclic graph-based ledgers instead of chained blocks and is called "Tangle". The strengths of IOTA include that it is a lightweight solution, as the transactions and consensus can be approved by communicating nodes; even two transactions can be verified by a single node and do not require the majority of communicating nodes to approve. No fee is required for the validation process, and thus no mining is required, which consequently reduces the overall compute power requirement for transactions. Every node submits the transaction information to the system using the Markov Chain Monte Carlo (MCMC) algorithm [45]. IOTA uses the Proof-of-Work (PoW) concept as a Sybil measure, which provides equal rights to all participants of the network for consensus and validation [46]. Practical applications of IOTA are discussed by Shabandri and Maheshwari [47] by proposing the use of IOTA for enhanced privacy and security of smart car meters. In contrast, a few

Table 11. Contingency table.

Challenges	Blockchain based solutions
Blockchain Integration Possibilities	0.968991428
Information Processing and Sourcing Blockchain-IoT	0.39689871
End to End Traceability	0.75038688
Anonymity and Data Privacy	0.024806076
Identity Management / Authentication	1.048062773
Confidentiality, Data Integrity, and Availability (CIA)	2.6062027
Chi Square is calculated as	34.77276669

researchers also conducted experimental assessments of IOTA on various platforms, discussing the issue that ledger size gets bigger and cannot be handled by IoT nodes, thus producing computational overhead [48]. Future development of the IoT architecture will overcome the limitation of large ledger sizes.

7.2 Ethereum

Ethereum, officially launched in 2015, is a Blockchain-based platform that offers support for different applications ranging from finance to IoT implementations. Ethereum is based on smart contract implementation, and these contracts are essentially programmed codes maintained permanently on the Blockchain network, enabling users to execute transactions. Ethereum offers the Ethereum Virtual Machine (EVM), which is essentially a decentralized virtual machine [49]. Ethereum uses smart contracts to keep transactions with different types of data, which provides great potential for IoT heterogeneous data. The only drawback Ethereum has is prolonged transmission time of more than 10 seconds. This limits real-time IoT applications from using Ethereum, as such long delays cannot be tolerated in time-constrained IoT applications. However, a few researchers have studied the implementation of IoT with Ethereum; for example, Sun et al. [50] proposed an Ethereum-based rich-thin-clients IoT solution that handles the issues pertaining to resource constraints in the mining of Blockchain with IoT.

7.3 VeChain

VeChain is a Distributed Ledger Technology (DLT), just like IOTA. VeChain is based on Geth, the Go implementation of the Ethereum protocol; however, it differs from the conventional algorithm of Ethereum by providing the "Proof-of-Authority" concept, which relies on authorized validators to secure the network [51]. VeChain was founded in 2015 to support supply chain management, logistics, and product life-cycle management operations. A common example of VeChain is "Thor," also called "VeThor" or "Thor Core," which stores supply-chain data and uses smart contracts for the execution of applications. A key feature of VeChain is its ability to allot unique identities to products in the supply chain and provide complete coverage and insights of the supply chain to the user. This functionality is implemented using RFIDs and NFCs on the products with IoT sensors to sense product locations. VeChain issues two types of tokens: VeChain Token (VET) and Thor Power (VTHO) for smart contract management. This two-token architecture provides a stable transaction fee mechanism; however, it may cause confusion among users and may limit the tokens' liquidity and adaptation.

7.4 WaltonChain

WaltonChain focuses mainly on RFID solutions, and it provides a decentralized Blockchain-based tamper-proof solution for sharing data in supply chains, just like VeChain. WaltonChain uses a dual consensus mechanism, i.e., Proof-of-Stake (PoS) and Proof-of-Work (PoW), which ensures energy efficiency as well as enhanced security in the network [52]. WaltonChain has a parent chain, also called the main chain, and sub-chains, i.e., child chains. The main chain manages various sub-chains, tracks transactions, executes smart contracts, and maintains the state of the sub-chains.

7.5 Hyperledger

Similar to IOTA and Ethereum, Hyperledger is an open-source Distributed Ledger Technology (DLT) platform. Hyperledger is a permissioned Blockchain technology, unlike Bitcoin or Ethereum, which are permissionless Blockchains, meaning that access is controlled by the network's governance rather than being open to all participants. This permissioned structure of Hyperledger enhances the security of the network by preventing Sybil attacks and reducing

the risks of malicious behaviour, which are common issues in permissionless systems. In Hyperledger, participants are known, and their roles are predefined, making it ideal for enterprise use cases where trust and control are crucial. Hyperledger differs from other conventional Blockchain systems mainly because of its permissioned model, which uses a more flexible consensus mechanism. It supports a variety of consensus protocols, including Practical Byzantine Fault Tolerance (PBFT), Raft, and other modular algorithms depending on the business case. Consensus in these mechanisms facilitates faster validations of transactions with higher throughput than in Proof-of-Work or Proof-of-Stake, rendering it more energy efficient and friendly to businesses for use-cases like IoT, supply chains, and finance. The smart contracts in Hyperledger are executed much faster, sometimes within milliseconds, which makes it a great candidate for real-time IoT applications requiring high-speed transactions. Beyond this, Hyperledger Fabric is one of the most widely adopted frameworks based on Hyperledger and is well suited to IoT implementations because it supports high throughput, low latency, and privacy features that are required in IoT environments. Studies comparing Ethereum and Hyperledger show that Hyperledger outperforms Ethereum by several orders of magnitude in terms of execution time and throughput. Performance analysis proved that Hyperledger is more scalable and allows for faster transaction validation than Ethereum, which is essential for the use cases that require real-time data processing and scalability [53].

7.6 HDAC

HDAC is designed for IoT applications using a permissioned Blockchain network that allows secure communication between devices. HDAC supports intermediary-enabled interoperability and connectivity between different Blockchain-based networks. HDAC uses quantum numbers, which provide enhanced security features essential for IoT applications (finance, e-commerce, healthcare, etc.) [54]. HDAC uses an enhanced Proof of Work (ePoW) consensus mechanism, which reduces energy consumption and makes it a more sustainable option for IoT networks with numerous devices.

Blockchain Platforms Comparison

The study of different Blockchain platforms and implementations reveals that IOTA, Ethereum, and Hyperledger are platforms that offer Blockchain functionalities and can be integrated with IoT architecture. However, Hyperledger Fabric, VeChain, WaltonChain, and HDAC are clear implementations of Blockchain with IoT. Such implementations are based on Blockchain platforms and further customized to meet certain business requirements. In this section, a comparison of Blockchain platforms is discussed; further integration of the platform is dependent on business needs and the specific use case of the IoT implementation. Comparison of Blockchain platforms for IoT depends on transaction speed, consensus mechanism, block sizes and capacity, scalability and interoperability, efficiency (performance as well as energy efficiency), security features, and future expandability. Every Blockchain platform offers certain strengths and weaknesses. To determine the best-suited Blockchain platform for a specific use case of IoT is dependent on critical analysis of required transaction speed, data security needs, energy efficiency, and interoperability, which are key considerations. As an example, a supply chain management application may require a highly secure and performance-efficient network to support a large number of transactions every second. A brief comparison of Blockchain platforms for IoT is discussed below:

7.6.1 Technology and Architecture:

IOTA is based upon unique architecture of Tangle using Directed Acyclic Graph (DAG) which differentiate it from traditional Blockchain by allowing fee-less transactions suited for IoT applications [55]. Ethereum uses execution of smart contracts and the development of Decentralized Applications (DApps) which shifts it from Proof-of-Work (PoW) to Proof-of-Stake (PoS) and thus addresses energy consumption issues [56]. Hyperledger includes various Blockchain technologies and tools, with Hyperledger Fabric as most popular implementation, is designed as permissioned network making it ideal for business-to-business (B2B) transactions and interoperability [57].

7.6.2 Scalability and Performance:

Comparison on the basis of scalability and performance of all three platforms reveals that both IOTA and Hyperledger outperforms Ethereum due to IOTA's DAG and Hyperledger permissioned model, providing faster transaction rate and greater scalability as compared to Ethereum [58].

7.6.3 Application and Adoption:

The adoption of Blockchain platforms are based upon specific business need and use-cases. IOTA is designed for fee-less fast micro-transactions in the IoT applications providing a direct machine-to-machine communication crucial for scalability of IoT ecosystem [5]9. Similarly, Ethereum is widely adopted for smart contract functionality supporting diverse range of applications beyond simple transactions such as decentralized finance (DeFi) and non-fungible tokens (NFTs) [60]. Hyperledger is a permissioned network supporting industrial applications from supply chain to digital identity due to its secure and scalable platform for private or consortium Blockchains [61].

7.7 Enhancing IoT Security through Blockchain Authentication:

The Blockchain technology, resolves some of the issues bordering the most nagging ones pertaining to the IoT ecosystem, specifically in the area of authentication and registration of device functionalities. However, the Blockchain technology cannot fix the vulnerabilities in the IoT devices, or even cannot try to fix the inherent flaws related to their security. But due to its potential, building up immutable and transparent records making it able noticeable improvement with credibility and security in the IoT ecosystems. As an example, the decentralization of the Blockchain allows tamper-proof and secure processes in authentication, enabling the possibility of reliable identification and authentication of every device within a network without any dependency on centralized authority. This controls the risk of spoofing, unauthorized access, and single point failure issues as few of the main pitfalls associated with IoT networks [62]. Alternative cryptographic approaches, such as Hyperelliptic Curve Cryptography (HECC), have also been explored for secure authentication in IoT environments, particularly in scenarios like Internet of Drones, where they offer comparable security with reduced computational overhead [68]. The inclusion of Blockchain technology enables easy and secure registration and management of IoT devices as it enables both verifiability and immutability in registrations, device configuration, and the transaction. Thus, gaining trust between devices in decentralized networks, as provenance of data integrity. Beside this, Blockchain technology offers smart contract automation making device interaction and its authorization processes easy further reducing the administrative overhead and increasing the operational efficiency of IoT systems [63].

7.8 Blockchain traits in IoT ecosystem:

Blockchain Technology (BCT) offers several traits that can significantly benefit the IoT ecosystem once deployed. These traits, such as decentralization, immutability, traceability, security, transparency, and smart contracts, can improve the overall efficiency and trustworthiness of IoT systems. For instance, decentralization allows IoT devices to communicate and process data without relying on a central authority, thus reducing the risk of a single point of failure. Additionally, immutability ensures that the data generated by IoT devices is tamper-proof, while traceability provides an audit trail of all transactions, enhancing data integrity. Furthermore, the integration of smart contracts into IoT systems can enable autonomous device interactions, where IoT devices can make decisions and execute actions based on pre-defined conditions, without human intervention. This can greatly improve the operational efficiency of IoT networks. However, deploying Blockchain within the IoT ecosystem comes with its challenges, such as resource constraints in IoT devices, network complexity, and energy consumption. Addressing these challenges is key to fully realizing the potential of BCT in IoT applications. Details of these traits include:

- Trackability and Traceability: Blockchain provides a transparent ledger where every transaction or data interaction is traceable, allowing for auditability and continuous monitoring of IoT devices. This is essential for ensuring data integrity and tracking the provenance of data from source to destination.
- Validation: IoT systems rely on Blockchain to ensure that all data generated by devices is valid. By using consensus algorithms (e.g., PoW, PoS), IoT networks can validate the authenticity of data without the need for a centralized authority, thereby ensuring that no unauthorized data enters the system.
- (Pseudo)Privacy: Blockchain can maintain privacy by using cryptographic methods such as public-private key encryption, enabling secure communication between devices while ensuring that sensitive information remains private. For example, IoT data may be stored transparently while personal data is encrypted, ensuring pseudo-privacy.
- Transparency and Accountability: With Blockchain, all data entries are immutable and visible to participants. This transparency

ensures accountability, as any attempt to alter data is easily detectable. For IoT, this feature is important for maintaining the trustworthiness of data generated by sensors, smart devices, or other networked devices.

- Governance (DAOs): Decentralized Autonomous Organizations (DAOs) allow for automated governance in IoT networks. Through smart contracts and voting mechanisms, DAOs provide autonomous decision-making and conflict resolution within decentralized IoT systems. This feature is especially useful in smart cities or other large-scale IoT implementations where centralized governance is impractical.
- Smart Contracts: Blockchain facilitates smart contracts, which are self-executing contracts with the terms of the agreement directly written into code. In IoT, smart contracts can automate interactions between devices (e.g., autonomous vehicles, smart meters), enabling devices to negotiate, validate transactions, and execute tasks without human intervention.

7.9 Blockchain as a Service (BaaS)

Blockchain as a Service (BaaS) is an emerging technology, offering scalable, secure and highly efficient framework for deployment of IoT applications over the cloud. Due to the complexity involved and requirement of in-depth knowledge of Blockchain technology for implementation, it usually costs higher to build, integrate and support the entire architecture locally. In order to reduce this effort, a cloud based "Blockchain as a Service" (BaaS) is introduced where the entire complexity of Blockchain is being implemented and managed centrally at high compute powered cloud and making it more accessible for businesses. BaaS offers full potential of Blockchain thus provides enhanced security, improved scalability, simplified integration, interoperability, data privacy and enablement for new businesses [61]. At present the BaaS architecture is being implemented and offered by different cloud service providers such as Amazon, Microsoft, IBM, Oracle and Ali Baba offering different implementations as per business requirements [64]. Moreover, a comparison of Blockchain based IoT implementation on local Fog computing vs. BaaS based implementation using cloud computing is discussed [65]. Study reveals that it's a trade-off between computational resources and latency. Fog computing, offers fast transactions at cost of limited compute power vs. Cloud based BaaS offers scalability at cost of latency. However, the integration of BaaS in IoT implementations not only mitigates the security, privacy and data related issues but also adds an additional layer of transparency and accountability for building trust among stakeholders. Thus, it provides verifiable and immutable record of transactions, ensures secure, authentic and tamper-proof data exchange within IoT network thus making it more resilient and trustworthy digital infrastructure.

8 Future Work

Artificial Intelligence (AI) and Quantum Computing are two major progressions that impend at the brink in the spectrum of Internet of Things (IoT) implementations and are likely to influence its arc dramatically in the continuum of Blockchain Technology. Integration of AI with Blockchain provides the potential to transform the functioning of systems in the IoT by enabling the systems for intelligent analysis of data, like that of enabling predictive maintenance and automatic systems of decision-making. Such a synergy is poised to allow better efficiencies in operations, fostering further data integrity, and nurturing innovative, smart, and secure IoT applications [62]. In addition, these smart contracts will automate very complex operations with the help of AI, adapt to patterns in data, and transact with the pinpoint accuracy and reliability as would arise from the integration of AI, improving the potential of IoT to manifolds [66]. Recent advances in anomaly detection for IoT leveraging machine learning techniques, combined with emerging 6G networks, demonstrate the potential for enhancing security and operational efficiency in IoT ecosystems through intelligent, real-time threat detection and response mechanisms [69]. Quantum-resistant cryptographic algorithms will represent an important field of research because the mission of such algorithms is to protect Blockchain from the clout of quantum attacks, thus enabling the possibility of sustaining the security of IoT ecosystems. This calls for preemptive establishment of quantum-proof Blockchain solutions; they should ensure post-quantum era implementation of the confidentiality, integrity, and overall trust of the information systems in an organization from IoT [67**?**]. The combination of Blockchain, AI, and Quantum Computing promises a totally new era for the IoT technology wrapped with three core aspects: security, efficiency, and intelligence. Futures research in this area will have to navigate judiciously the developments and use AI analytical abilities in order to optimize the

capabilities of Blockchain networks. This approach is going to solve not only the contemporary issues of IoT implementations but also introduce further dimensions to it, including utility, scalability, and resilience in the interconnected world.

9 Conclusion

In conclusion, this systematic review demonstrates that the integration of Blockchain Technology (BCT) with the Internet of Things (IoT) is not merely an incremental enhancement but a foundational evolution required to address the inherent security, privacy, and scalability limitations of traditional centralized IoT architectures. Through a rigorous review of 86 scholarly articles, this paper has shown that the core attributes of blockchain—decentralization, immutability, and transparency—directly counter the most pressing vulnerabilities in the IoT ecosystem, such as single-point failures and data integrity breaches. The use of a Chi-square test provided statistical validation for this claim, revealing a strong and significant association in the academic literature between the challenges of IoT and the proposal of blockchain-based solutions.

The practical deployment of BCT in IoT, however, requires careful consideration of the diverse platforms and architectures available. This review has provided a critical comparative analysis of leading platforms like Ethereum, Hyperledger Fabric, and IOTA, highlighting their distinct trade-offs in performance, governance, and energy efficiency. This analysis, supplemented with real-world case studies in healthcare, smart cities, and supply chain management, offers a strategic guide for practitioners to select the platform best suited to their specific application requirements. While Ethereum excels in smart contract functionality, its scalability and cost issues limit its use in many IoT contexts. Hyperledger Fabric offers a high-performance, private solution for enterprise needs, whereas IOTA's innovative Tangle architecture presents a theoretically ideal model for a feeless, scalable machine-to-machine economy.

Despite the clear benefits, the path to widespread adoption is not without challenges. Issues of network latency, the computational constraints of IoT devices, and the energy consumption of certain consensus mechanisms like Proof-of-Work must be continually addressed through the development of lightweight algorithms and innovative platforms. As this digital era advances, the integration of emerging technologies such as AI and 6G with blockchain-secured IoT networks will pave the way for more intelligent, efficient, and highly scalable solutions. This research contributes to the academic discourse by providing a robust framework for understanding the Blockchain-IoT synergy and lays a solid foundation for future explorations in this transformative domain, ensuring a more secure and trustworthy future for our increasingly interconnected world.

Data Availability Statement

Not applicable.

Funding

This work was supported without any funding.

Conflicts of Interest

The authors declare no conflicts of interest.

AI Use Statement

The authors declare that no generative AI was used in the preparation of this manuscript.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] Loukil, F., Ghedira-Guegan, C., Benharkat, A. N., Boukadi, K., & Maamar, Z. (2017, October). Privacy-aware in the IoT applications: a systematic literature review. In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"* (pp. 552-569). Cham: Springer International Publishing. [CrossRef]

[2] Xue, M., Papadimitriou, P., Raïssi, C., Kalnis, P., & Pung, H. K. (2011, April). Distributed privacy preserving data collection. In *International Conference on Database Systems for Advanced Applications* (pp. 93-107). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[3] Atlam, H. F., Alenezi, A., Walters, R. J., Wills, G. B., & Daniel, J. (2017, June). Developing an adaptive Risk-based access control model for the Internet of Things. In *2017 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)* (pp. 655-661). IEEE. [CrossRef]

[4] Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology

and standardization. *Wireless personal communications, 58*(1), 49-69. [CrossRef]

[5] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad hoc networks, 10*(7), 1497-1516. [CrossRef]

[6] Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review, 26*(1), 23-30. [CrossRef]

[7] Jain, A., Sharma, B., & Gupta, P. (2016). Internet of things: Architecture, security goals, and challenges—A survey. *International journal of innovative research in science and engineering, 2*(4), 154-163.

[8] Alfaqih, T. M., & Al-Muhtadi, J. (2016). Internet of things security based on devices architecture. *International Journal of Computer Applications, 133*(15), 19-23. [CrossRef]

[9] Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Intelligence of things: opportunities & challenges. *2018 3rd Cloudification of the Internet of Things (CIoT)*, 1-6. [CrossRef]

[10] Conoscenti, M., Vetro, A., & De Martin, J. C. (2017, May). Peer to peer for privacy and decentralization in the internet of things. In *2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)* (pp. 288-290). IEEE. [CrossRef]

[11] Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Fog computing and the internet of things: A review. *Big Data and Cognitive Computing, 2*(2), 10. [CrossRef]

[12] Biswas, K., & Muthukkumarasamy, V. (2016, December). Securing smart cities using blockchain technology. In *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)* (pp. 1392-1393). IEEE. [CrossRef]

[13] Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. *Journal of electrical and computer engineering, 2017*(1), 9324035. [CrossRef]

[14] Kumar, N. M., & Mallick, P. K. (2018). The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. *Procedia computer science, 132*, 109-117. [CrossRef]

[15] Fabiano, N. (2017, June). Internet of Things and blockchain: Legal issues and privacy. The challenge for a privacy standard. In *2017 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)* (pp. 727-734). IEEE. [CrossRef]

[16] Chatterjee, J. M., Kumar, P. S., Kumar, A., & Balamurugan, B. (2020). Blockchain, Bitcoin, and the Internet of Things: Overview. *Blockchain Technology and the Internet of Things*, 47-67.

[17] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved July 10, 2025, from https://bitcoin.org/en/bitcoin-paper

[18] Sultan, K., Ruhi, U., & Lakhani, R. (2018). Conceptualizing Blockchains: Characteristics & applications. *arXiv preprint arXiv:1806.03693*.

[19] Wu, H., Li, Z., King, B., Ben Miled, Z., Wassick, J., & Tazelaar, J. (2017). A distributed ledger for supply chain physical distribution visibility. *Information, 8*(4), 137. [CrossRef]

[20] Leva, A., Strada, S., & Tanelli, M. (2019, June). Control-oriented modelling of proof-of-work blockchains. In 2019 18th European Control Conference (ECC) (pp. 2873-2878). IEEE. [CrossRef]

[21] Miraz, M. H., & Ali, M. (2020). Integration of blockchain and IoT: an enhanced security perspective. *arXiv preprint arXiv:2011.09121*.

[22] Atlam, H. F., & Wills, G. B. (2019). An efficient security risk estimation technique for Risk-based access control model for IoT. *Internet of Things, 6*, 100052. [CrossRef]

[23] Banafa, A. (2017). Three major challenges facing iot. *IEEE Internet of Things*, 26-67.

[24] Alkurdi, F., Elgendi, I., Munasinghe, K. S., Sharma, D., & Jamalipour, A. (2018, November). Blockchain in IoT security: A survey. In *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)* (pp. 1-4). IEEE. [CrossRef]

[25] Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in internet of things: challenges and solutions. *arXiv preprint arXiv:1608.05187*.

[26] Khan, M. A., & Salah, K. (2018). IoT security: Review, Blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395-411. [CrossRef]

[27] Hang, L., & Kim, D. H. (2019). Design and implementation of an integrated iot Blockchain platform for sensing data integrity. *Sensors, 19*(10), 2228. [CrossRef]

[28] Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and iot integration: A systematic survey. *Sensors, 18*(8), 2575. [CrossRef]

[29] Polyzos, G. C., & Fotiou, N. (2017, August). Blockchain-assisted information distribution for the Internet of Things. In *2017 IEEE International Conference on Information Reuse and Integration (IRI)* (pp. 75-78). IEEE. [CrossRef]

[30] Mahmood, M. S., & Al Dabagh, N. B. (2023). Blockchain technology and internet of things: review, challenge and security concern. *International Journal of Electrical and Computer Engineering, 13*(1), 718-735. [CrossRef]

[31] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation*

Computer Systems, 78, 544-546. [CrossRef]

[32] Tandon, A. (2019). An empirical analysis of using blockchain technology with internet of things and its application. Int. J. Innov. Technol. *Explor. Eng, 8*(9), 1470-1475. [CrossRef]

[33] Zhu, X., & Badr, Y. (2018). Identity management systems for the internet of things: A survey towards Blockchain solutions. *Sensors, 18*(12), 4215. [CrossRef]

[34] Kadam, S. B., & John, S. K. (2020). Blockchain integration with low-power internet of things devices. In *Handbook of Research on Blockchain Technology* (pp. 183-211). Academic Press. [CrossRef]

[35] Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE internet of things journal, 5*(2), 1184-1195. [CrossRef]

[36] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the internet of things. IEEE Access, 6, 32979-33001. [CrossRef]

[37] Badr, S., Gomaa, I., & Abd-Elrahman, E. (2018). Multi-tier Blockchain framework for IoT-EHRs systems. *Procedia Computer Science, 141*, 159-166. [CrossRef]

[38] Patil, A. S., Tama, B. A., Park, Y., & Rhee, K. H. (2017, December). A framework for blockchain based secure smart green house farming. In *International Conference on Ubiquitous Information Technologies and Applications* (pp. 1162-1167). Singapore: Springer Singapore. [CrossRef]

[39] Kamilaris, A., Fonts, A., & Prenafeta-Boldý, F. X. (2019). The rise of Blockchain technology in agriculture and food supply chains. *Trends in Food Science & Technology, 91*, 640-652. [CrossRef]

[40] Rejeb, A., Keogh, J. G., & Treiblmaier, H. (2019). Leveraging the internet of things and Blockchain technology in supply chain management. *Future Internet, 11*(7), 161. [CrossRef]

[41] Zhang, Y., & Wen, J. (2017). The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications, 10*(4), 983-994. [CrossRef]

[42] Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal, 6*(5), 8076-8094. [CrossRef]

[43] Rahman, M. S., Chamikara, M. A. P., Khalil, I., & Bouras, A. (2022). Blockchain-of-blockchains: An interoperable blockchain platform for ensuring IoT data integrity in smart city. *Journal of Industrial Information Integration, 30*, 100408. [CrossRef]

[44] Rani, S., Kataria, A., Sharma, V., Ghosh, S., Karar, V., Lee, K., & Choi, C. (2021). Threats and corrective measures for IoT security with observance of cybercrime: A survey. *Wireless communications and mobile computing, 2021*(1), 5579148. [CrossRef]

[45] Raschendorfer, A., Mörzinger, B., Steinberger, E., Pelzmann, P., Oswald, R., Stadler, M., & Bleicher, F. (2019). On IOTA as a potential enabler for an M2M economy in manufacturing. *Procedia CIRP, 79*, 379-384. [CrossRef]

[46] Douceur, J. R. (2002, March). The sybil attack. In *International workshop on peer-to-peer systems* (pp. 251-260). Berlin, Heidelberg: Springer Berlin Heidelberg. [CrossRef]

[47] Shabandri, B., & Maheshwari, P. (2019, March). Enhancing IoT security and privacy using distributed ledgers with IOTA and the tangle. In *2019 6th International conference on signal processing and integrated networks (SPIN)* (pp. 1069-1075). IEEE. [CrossRef]

[48] Atlam, H. F., Azad, M. A., Alzahrani, A. G., & Wills, G. (2020). A Review of Blockchain in Internet of Things and AI. *Big Data and Cognitive Computing, 4*(4), 28. [CrossRef]

[49] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper, 151*(2014), 1-32.

[50] Sun, H., Hua, S., Zhou, E., Pi, B., Sun, J., & Yamashita, K. (2018, June). Using ethereum blockchain in Internet of Things: A solution for electric vehicle battery refueling. In *International Conference on Blockchain* (pp. 3-17). Cham: Springer International Publishing. [CrossRef]

[51] Bischoff, O., & Seuring, S. (2021). Opportunities and limitations of public blockchain-based supply chain traceability. *Modern Supply Chain Research and Applications, 3*(3), 226-243. [CrossRef]

[52] Li, Z., Wang, W. M., Liu, G., Liu, L., He, J., & Huang, G. Q. (2018). Toward open manufacturing: A cross-enterprises knowledge and services exchange framework based on blockchain and edge computing. *Industrial Management & Data Systems, 118*(1), 303-320. [CrossRef]

[53] Pongnumkul, S., Siripanpornchana, C., & Thajchayapong, S. (2017, July). Performance analysis of private Blockchain platforms in varying workloads. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-6). IEEE. [CrossRef]

[54] Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access, 8*, 21091-21116. [CrossRef]

[55] Popov, S. (2018). The tangle. *White Paper, 1*(3), 30.

[56] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *White Paper, 3*(37), 2-1.

[57] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth EuroSys conference* (pp. 1-15). [CrossRef]

[58] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352-375. [CrossRef]

[59] Makhdoom, I., Abolhasan, M., & Ni, W. (2018, January). Blockchain for IoT: The challenges and a way forward. In *ICETE 2018-Proceedings of the 15th International Joint Conference on e-Business and Telecommunications*. [CrossRef]

[60] Wohrer, M., & Zdun, U. (2018, March). Smart contracts: security patterns in the ethereum ecosystem and solidity. In *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)* (pp. 2-8). IEEE. [CrossRef]

[61] Gascon-Samson, J., Rafiuzzaman, M., & Pattabiraman, K. (2017, December). Thingsjs: Towards a flexible and self-adaptable middleware for dynamic and heterogeneous iot environments. In *Proceedings of the 4th Workshop on Middleware and Applications for the Internet of Things* (pp. 11-16). [CrossRef]

[62] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On Blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems, 88*, 173-190. [CrossRef]

[63] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4*, 2292-2303. [CrossRef]

[64] Song, J., Zhang, P., Alkubati, M., Bao, Y., & Yu, G. (2022). Research advances on blockchain-as-a-service: Architectures, applications and challenges. *Digital Communications and Networks, 8*(4), 466-475. [CrossRef]

[65] Samaniego, M., Jamsrandorj, U., & Deters, R. (2016, December). Blockchain as a Service for IoT. In *2016 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)* (pp. 433-436). IEEE. [CrossRef]

[66] Singh, S. K., Rathore, S., & Park, J. H. (2020). Blockiotintelligence: A Blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Generation Computer Systems, 110*, 721-743. [CrossRef]

[67] Sandner, P., Gross, J., & Richter, R. (2020). Convergence of Blockchain, IoT, and AI. *Frontiers in Blockchain, 3*, 522600. [CrossRef]

[68] Khan, M. A., Ullah, I., Alkhalifah, A., Rehman, S. U., Shah, J. A., Uddin, M. I., ... & Algarni, F. (2021). A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems. *IEEE Transactions on Industrial Informatics, 18*(5), 3416-3425. [CrossRef]

[69] Saeed, M. M., Saeed, R. A., Abdelhaq, M., Alsaqour, R., Hasan, M. K., & Mokhtar, R. A. (2023). Anomaly detection in 6G networks using machine learning methods. *Electronics, 12*(15), 3300. [CrossRef]

M Khurram Umair Postgraduate student at University of Engineering and Technology, Peshawar. Currently pursuing his postgraduate studies in the field of Computer Science, M. Khurram Umair is an emerging researcher affiliated with the University of Engineering and Technology in Peshawar, Pakistan. (Email: umair19@hotmail.com)

Dr. Mohammad Sohail Khan is an Assistant Professor in the Department of Computer Software Engineering at the University of Engineering and Technology, Mardan. He has a background as a software engineer and has held several academic and administrative roles. Dr. Khan earned his Ph.D. in Computer Engineering from Jeju National University in South Korea and focuses his research on Artificial Intelligence, Machine Learning, and the Internet of Things. (Email: sohail.khan@uetmardan.edu.pk)

Muhammad Faisal Abrar is currently an Assistant Professor with the College of Computer Science and Engineering, University of Hai'l, Saudi Arabia. His research interests include agile software development, software quality assurance, software outsourcing partnership, empirical software engineering, systematic literature review, big data, the Internet of Things, and information sciences. He has also acted as a Reviewer of esteemed international journals, such as Complex & Intelligent Systems (CAIS), Information Sciences, IEEE Access, Scientific Programming, Electronics, Mobile Information Systems, and Journal of Software: Evolution and Process. (Email: m.abrar@uoh.edu.sa)