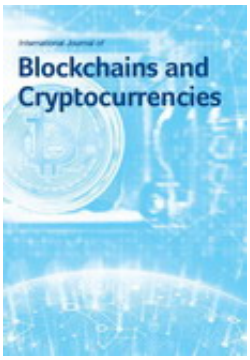
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Blockchains and Cryptocurrencies

ISSN online: 2516-6433 - ISSN print: 2516-6425
https://www.inderscience.com/ijbc

Blockchain in the IoT: security, applications, technologies, and challenges

Mahd M. Alzoubi

DOI: 10.1504/IJBC.2024.10063367

Article History:

Received:	15 November 2023
Last revised:	02 March 2024
Accepted:	04 March 2024
Published online:	26 July 2024

Blockchain in the IoT: security, applications, technologies, and challenges

Mahd M. Alzoubi

Department of Cybersecurity and Information Technology,
University of West Florida,
11000 University Parkway,
Building 4, Office 436B,
Pensacola, FL, 32514, USA
Email: malzoubi@uwf.edu

Abstract: This paper explores the potential of blockchain technology to enhance the security and trust of the Internet of Things (IoT) ecosystem. It identifies key challenges faced by IoT applications, such as data privacy, security, and interoperability. The paper then analyses how blockchain's characteristics, including decentralisation, immutability, and transparency, offer solutions to these challenges. It highlights how blockchain can secure data transactions, automate device authentication, and ensure data integrity, addressing critical IoT vulnerabilities. However, the paper acknowledges the complexities of integrating blockchain and IoT (BCIoT), including scalability limitations, energy consumption concerns, and the need for interoperability across diverse platforms. Additionally, regulatory considerations surrounding blockchain's decentralised nature are discussed. The paper concludes by emphasising the contribution of this research in providing a comprehensive analysis of blockchain's potential to secure, streamline, and manage IoT applications, paving the way for their secure and efficient integration.

Keywords: blockchain; IoT; security; smart contracts; consensus algorithms: privacy; trust.

Reference to this paper should be made as follows: Alzoubi, M.M. (2024) 'Blockchain in the IoT: security, applications, technologies, and challenges', *Int. J. Blockchains and Cryptocurrencies*, Vol. 5, No. 1, pp.14–43.

Biographical notes: Mahd M. Alzoubi is a Member of the Faculty at the University of West Florida's Department of Cybersecurity and Information Technology. Holding a PhD in Information Systems, a Master of Science in Computer Science, and a Bachelor of Science in Computer Science, he brings a rich educational background and over 18 years of teaching experience to the classroom. His academic journey and professional dedication have firmly established him as an expert in his field. At the heart of his research endeavours are enterprise systems, cybersecurity, cloud computing, and blockchain technology. Through his scholarly work, he aims to contribute to the advancement of these fields, addressing current challenges and exploring future possibilities. His research is driven by a passion for innovation and a commitment to excellence.

1 Introduction

The integration of Blockchain and the Internet of Things (IoT) can change how we interact with technology. IoT connects all things via the internet, which involves using software, sensors, actuators, and connectivity devices to enable communication, data collection, and data exchange among various integrated devices, such as vehicles, home appliances, and other products. On the other hand, Blockchain (BC) focuses on maintaining the infrastructure's reliability, immutability, and trust (Alam et al., 2023). The rapid expansion of IoT technology introduces significant challenges, including concerns over data privacy, security, management, and interoperability. For example, IoT data, particularly in intelligent healthcare systems, contains critical and confidential information, with IoT devices attached to patients collecting sensitive health data for continuous monitoring and emergency alerts. The security of these devices and the information they transmit is essential, as medical decisions rely on this accurately sensed and transmitted data (Khashan and Khafajah, 2023). This raises the risk of severe security breaches and privacy issues, leading to system and widespread data communication failures. These issues underscore the urgent need for IoT solutions incorporating strong security and privacy measures to prevent the failure of IoT deployments across various sectors. Blockchain technology emerges as a promising solution to strengthen IoT security through its capabilities for secure access control, data sharing management, and identity verification. By adopting Blockchain, IoT systems can overcome the limitations of traditional centralised models by ensuring higher levels of availability, transparency, and security over distributed architectures, enhanced data integrity, decentralised processing, and the facilitation of smart contracts (Albulayhi and Alsukayti, 2023). In recent years, there has been an increasing interest in the integration of these two technologies to create new solutions for a wide range of industries (Hemdan et al., 2023; Tripathi et al., 2023).

Blockchain technology is a peer-to-peer (P2P) digital ledger that is both distributed and decentralised. The term 'blockchain' suggests that data blocks are encrypted using a hashing algorithm and then chained together through a consensus mechanism to form the Blockchain (Alzoubi, 2021). This technology helps provide trust, eliminates third-party trust vendors, and reduces transaction times and associated costs. Blockchain provides security through cryptography (hashing algorithms), immutability, distributed nature, and the ability to store information without being tampered with (Yaga et al., 2019). According to Hedge et al. (2023), Blockchain can significantly transform various sectors and the IoT by offering decentralised frameworks that result in more secure, transparent, and efficient systems. As the number of connected IoT devices grows, the data generated by these devices also grows. The large amounts of data generated by several other devices, such as surveillance cameras, sensors, and healthcare data, need better management and security. Cecilia Eberendu and Ifeanyi Chinebu (2021) stated that "IoT interconnects people and things anytime, anywhere with anything and anyone using available network and service and involves a device that can sense, actuate and communicate to link information and physical world. The purpose of IoT is to connect things (devices, communication, and services) anytime, anywhere with anyone using networks" (p.123). Global data traffic has increased unprecedentedly over the last decade; thus, the interest in utilising IoT devices is becoming more evident in various industries and residential. IoT devices and their usage have various benefits. However, they show many security gaps and are thus vulnerable to attacks, data theft, and fraud.

According to Dorri et al. (2017), traditional security mechanisms, such as firewalls and encryption, are no longer sufficient to address the sophisticated attacks and vulnerabilities associated with IoT devices. This has led to exploring blockchain technology as a potential solution to enhance IoT security. Alam et al. (2023) noted that IoT devices share a large amount of space between different devices over a common platform called IoT. The IoT platform allows different applications to communicate by combining data from different devices and applying analytics on the data to share valuable information. In addition, the author also suggested that smart devices in our houses are connected to the smart hub, which contains significant vulnerabilities for hackers. Blockchain technology has emerged as a potential solution to these challenges, offering a decentralised and secure way to store and exchange data. This literature review explores the intersection of IoT and Blockchain and the current state of research in this area.

The motivation behind integrating Blockchain with IoT is established from the urgent need to address the growing concerns about data security, management, and efficiency in IoT systems. As the IoT continues to expand, the vulnerabilities associated with IoT devices and networks become more evident due to the limitations of traditional security mechanisms. Blockchain technology, with its decentralisation, immutability, and cryptographic security features, presents an advanced approach to addressing these challenges. Blockchain, as a solution for enhancing IoT security and efficiency, is derived from the potential to adopt a more secure, transparent, and efficient digital environment (Hemdan et al., 2023). This integration aims to mitigate the risks associated with IoT devices and unlock innovation opportunities across various industries. This paper contributes to the ongoing research on integrating Blockchain technology with IoT by providing a comprehensive review and analysis of blockchain solutions to the challenges in the IoT domain. It offers an in-depth overview of Blockchain and IoT (BCIoT), surveying various blockchain solutions that address crucial issues such as security, data management, and efficiency within the IoT environment. In addition to highlighting the potential benefits of this integration, the paper sheds light on the significant advancements that can be achieved. However, it also acknowledges the existing challenges, such as scalability and interoperability, physical attacks with the deployed IoT devices and malware injection, DDoS attacks, and battery drainage attacks, among others, that need to be addressed to fully realise the potential of BCIoT convergence (Adhikari and Ramkumar, 2023). This research contributes valuable understanding and guidance for industries seeking to leverage these technologies for enhanced security, efficiency, transparency, and trust.

2 Related content

2.1 Blockchain architecture and applications

This section introduces the relevant literature on BCIoT. Blockchain was initially invented for Bitcoin, but its applications have gone beyond cryptocurrencies. A blockchain is a data structure that maintains the connection between data stored across a distributed network. This data is organised into interconnected blocks within a collective ledger (ElGayyar et al., 2020). Hedge et al. (2023) present an extensive survey on the integration of BCIoT in healthcare, addressing the need to enhance data security, privacy, and other challenges faced by traditional IoT medical services. It offers a detailed

examination of BCIoT technologies and their role in healthcare applications like remote patient monitoring and electronic health record management. The study underscores the potential of BCIoT to improve patient care and outlines future directions for advancing healthcare services. Yang et al. (2020) discusses the use of blockchain technology in IoT security and data management. The author also discusses the benefits of a blockchain approach to secure IoT applications. Wang et al. (2021) overviewed the existing blockchain solutions for IoT applications. They analysed the consensus protocols of Blockchain that are suitable for IoT applications. Zhang et al. (2020) reviewed blockchain-based security architecture for the IoT. The authors concluded that Blockchain could use distributed data storage, consensus mechanisms, point-to-point transmission, and encryption algorithms to solve IoT security problems. The authors suggested that public Blockchain makes the system more scalable and functional, and sending messages in private Blockchain can only be performed by a consensus group. Rahman et al. (2022) present a thorough survey on the emerging applications of Blockchain (BC) technology in healthcare, highlighting its integration with the IoT to enhance scalability and maintain data consistency in a decentralised manner. It outlines the applications, research issues, security threats, challenges, opportunities, and prospects of BC technologies in IoT-enabled healthcare systems, mainly focusing on the privacy and storage of medical records. Additionally, the paper evaluates state-of-the-art BC implementations in the medical field, detailing their advantages and disadvantages, and offers guidance for future research to address the limitations of existing studies.

Researchers have been exploring various applications of this combination, ranging from supply chain management to energy distribution. For example, a study by Zhang et al. (2021) proposed a blockchain-based framework for smart manufacturing in IoT environments. The framework utilised blockchain technology to provide secure and transparent data sharing between manufacturing processes, allowing for greater efficiency and reduced costs. It offers substantial cost benefits by automating processes and reducing the need for intermediaries, thereby lowering operational costs. It enhances security, mitigating the costs associated with data breaches and fraud. Blockchain's transparency and traceability improve supply chain management, reducing losses and inventory costs. The shift to energy-efficient consensus mechanisms like proof of stake (PoS) reduces energy costs, which is especially beneficial for energy-constrained IoT devices.

Additionally, Blockchain's decentralised nature decreases maintenance costs associated with centralised data storage and enhances interoperability among IoT devices, leading to long-term savings by easing the integration of diverse technologies. This integration streamlines operations, enhances security, and promotes efficient resource management, ultimately significantly reducing costs for businesses and consumers. (Behera et al., 2023) Conclude that blockchain technology is a transformative force in the software industry, offering significant improvements to supply chain management. It highlights Blockchain's ability to enhance transparency, accountability, and trust, particularly for valuable goods like diamonds, gold, liquor, and medical drugs. By removing intermediaries, Blockchain reduces costs and delivers a secure, transparent system capable of preemptively addressing potential issues when integrated with radio-frequency identification (RFID) technology in IoT.

Another area of interest in the intersection of IoT and Blockchain is in the field of healthcare. Using blockchain technology in healthcare can provide benefits such as secure and transparent patient data sharing, improved supply chain management, and the

automation of administrative tasks. A study by Raj and Prakash (2023) proposed a blockchain-based framework for medical data sharing in IoT environments. The authors introduce a transparent, tamper-proof, distributed, and decentralised innovative healthcare system (DSHS) employing blockchain-based smart contracts. Utilising an immutable modified Merkle tree structure, the system secures transactions for viewing contracts on a public blockchain, updates patient health records (PHR), and facilitates PHR exchange among all relevant entities.

Blockchain uses several participating nodes to initiate a transaction using private key cryptography. A transaction represents the transfer of digital assets between multiple peers on the distributed networks. Transactions are stored in a pool and disseminated in the chain using the Gossip protocol. The participating members have complete authority to monitor all transactions in the blockchain network in a P2P network. Subsequently, peers need to validate these transactions based on some coded conditions. After the miners verify and validate the transaction, it is added to the block. Blockchain technology comprises a list of records commonly known as blocks wherein the information stored is distributed and encrypted, ensuring privacy and security (Chowdhury et al., 2023; Alzoubi, 2021). The sequence of blocks maintains the information of all transactions and are linked to each other via a reference hash. The first block in the Blockchain is called the genesis block. Each block in the Blockchain consists of the block header and the block body. Blockchain presents a decentralised, shared platform that provides transparency and immutability of all transactions. The nodes give the service for linking the blocks to each other. Each block contains the previous block hash function to create and maintain a blockchain (Gad et al., 2022). Each node in the transaction has a public key infrastructure (PKI) private key and public key pair. Transactions are signed using the private key and later confirmed with the public key. The transactions are sent to all participating nodes using a consensus method. The nodes agree on the validation of each transaction (Gad et al., 2022). When a node in the network wants to ensure consistency of transactions, it compares its Merkle root with every other node's Merkle root transactions in the current block. Merkel tree is a cryptographic tool that summarises all the transactions in a block, allowing for efficient and secure verification of large datasets in a blockchain. Each block is made up of two components, namely, the block header and the block data. The block header contains metadata, such as the unique block identifier, the hash value of the previous block to which it will be chained, a hash output of block data, block size, the nonce value, and a timestamp. The block data consists of transaction information recorded on the block (Tripathi et al., 2023; Gad et al., 2022; Alzoubi, 2021). The diagram below shows the summarised components of Blockchain.

The expression below represents the process of hashing the processed data from each block in the Blockchain and then concatenating those hashes to form a single hash that represents the entire Blockchain. This hash example verifies the integrity of the Blockchain and ensures that it has not been tampered with (Nakamoto, 2008; Narayanan et al., 2016).

Let H(n) be the hash function used in the Blockchain, where n is the input data.

Let P(n) be the processing function that processes the input data before hashing.

Let b_i be the ith block in the Blockchain, where i = 1, 2, ..., m.

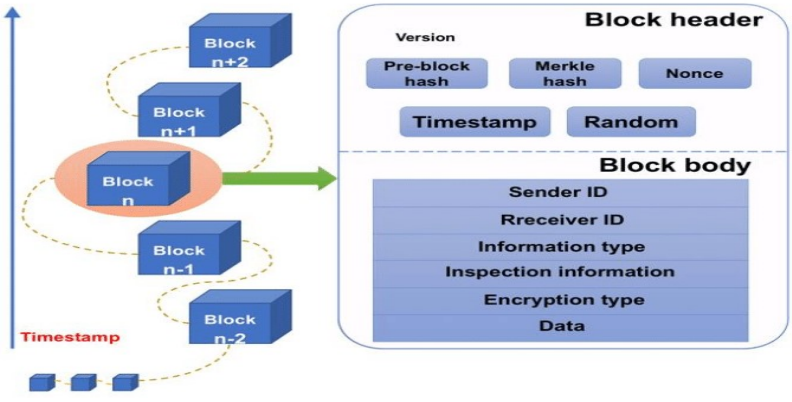
Let D_i be the data stored in block b_i.

The transformation and subsequent hashing of data within a blockchain network can be conceptualised and represented through the following mathematical expression:

H (P(D1)//P(D2)//.../P(Dm)) where "||" denotes concatenation.

The result of this operation is a single hash value that uniquely represents the processed data of the entire Blockchain up to the *m*th block. Any change in any of the data blocks, even a minor one, would result in a drastically different hash value when this process is repeated. This property is fundamental in Blockchain for ensuring data integrity: one can quickly check if data has been altered or tampered with by comparing the expected hash value with the one calculated from the current data.

Figure 1 Blockchain architecture (see online version for colours)



Source: Gu et al. (2020)

2.2 Blockchain characteristics

As explained by Tripathi et al. (2023) and Alzoubi (2021), blockchain technology represents a significant shift in how data is stored, managed, and verified across various sectors. This distributed digital ledger technology eliminates the need for centralised control, instead relying on a network of nodes to validate and record transactions in a secure, transparent, and immutable manner. Alzoubi (2021) emphasises the core characteristics that make Blockchain an innovative technology:

- *Decentralisation*: Unlike traditional systems that rely on a central authority, Blockchain operates on a distributed ledger that enhances processing capabilities, reduces latency, and removes single points of failure, thereby increasing the system's strength.
- *Immutability*: Once a transaction is recorded in a block and added to the chain, it cannot be altered. This feature ensures the integrity of the transaction history, making Blockchain a trustworthy platform for recording transactions.
- *Transparency*: The transparency of blockchain technology is unparalleled. Since every transaction is recorded on a ledger that's accessible to all network participants, it ensures that all transactions are visible and verifiable by anyone, thereby promoting trust among users.

- *Security*: Blockchain's use of cryptographic principles, such as PKI, safeguards against unauthorised data modifications. This level of security is vital in preventing fraud and malicious attacks.
- *Efficiency*: By distributing its database records across a network of users, blockchain technology allows for the verification of all records stored in the database, streamlining transactions and enhancing overall efficiency.
- *Privacy and resilience*: Among various cryptographic protocols, Blockchain also significantly enhances user privacy. The redundancy built into the blockchain system makes it exceptionally resilient and immutable, further solidifying its reliability as a digital ledger system.

Tripathi et al. (2023) and Alzoubi (2021) portrayed a comprehensive picture of Blockchain as a technology and a paradigm shift in digital transactions and data management. The decentralised, immutable, transparent, secure, and efficient nature of Blockchain redefines concepts of trust, ownership, identity, and financial systems, offering a pseudo-anonymous solution that promises to profoundly reshape industries and commerce. This technology's inherent attributes suggest a future where digital transactions and records are conducted with unprecedented levels of security, transparency, and trust, marking a significant departure from traditional centralised systems. Moreover, Blockchain also strengthens privacy through different cryptographic protocols. Redundancy in Blockchain makes the system very resilient and immutable.

2.3 A summary of key elements and innovations in blockchain technology

In the study of architecture and advancements in blockchain technology, several key elements and innovations are forming the base of this technology (Alam, 2022). At the core of blockchain functionality are transactions, which signify digital exchanges related to tangible and digital assets among network participants. These transactions are collated into blocks, contributing to the overall structure of the Blockchain.

Integral to transaction security is the digital signature, a mechanism that verifies the authenticity of digital messages by ensuring they remain unaltered during transit and establishing their provenance. Meanwhile, the introduction of sharding partitions the blockchain storage into more manageable segments or 'shards', enhancing both efficiency and security without compromising the integrity of the data.

Smart contracts have emerged as a pivotal innovation, enabling the execution of contractual terms directly on the Blockchain when specific conditions are pre-satisfactorily met, thereby bypassing traditional intermediaries, and expediting operations. Complementing this is the Merkle Tree, a cryptographic tool that succinctly aggregates all transactions in a block, facilitating the swift and secure verification of large datasets within the Blockchain (Tsai and Shen, 2024; Alzoubi, 2021). Furthermore, the process of hashing is fundamental, transforming any input into a consistent, encrypted output size – crucial for the blockchain network's operational integrity. Overlaying these technical components is the array of consensus algorithms, which are imperative for aligning all network nodes on a single, verified data version – underscoring the dependability and security of distributed ledgers. Hussein et al. (2023) noted that in the context of the IoT, the transition from proof of work (PoW) to PoS in blockchain technology holds significant implications for enhancing security, efficiency, and

scalability. IoT devices, often constrained by limited computational resources, energy capacity, and bandwidth, can significantly benefit from adopting PoS due to its lower energy consumption compared to the computationally intensive PoW. This makes PoS particularly suitable for IoT ecosystems, where energy efficiency is vital. The landscape of consensus algorithms is further diversified with variations such as delegated proof of stake (DPoS), where stakeholders elect representatives to undertake validation on their behalf; leased proof of stake (LPoS), which enables coin holders to lease their stakes to augment the chances of validators being chosen; proof of elapsed time (PoET), which promotes fairness in block validation by implementing a randomised waiting period; and practical Byzantine fault tolerance (PBFT), designed to achieve consensus even amid potentially harmful nodes, thus enhancing the fault tolerance and security of the system. Each of these algorithms contributes uniquely to the strength and efficiency of blockchain networks, ensuring their viability in an increasingly digitised economy (Tripathi et al., 2023; Popoola et al., 2023; Zhong et al., 2023).

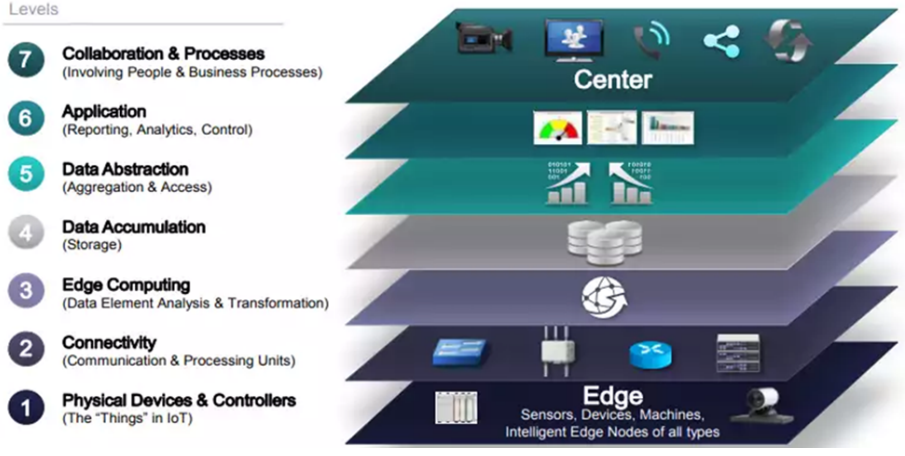
2.4 IoT applications and services

IoT applications have increased in recent years and play a vital role in telecommunication services. The IoT has been implemented in many application domains, such as smart homes, healthcare, and vehicles. IoT devices perform security-critical operations, such as monitoring and storing sensitive information. As such, IoT-based systems are of great interest to attackers. Through the connection of vehicles, appliances, and many other electronic devices to the internet, IoT will provide convenient living environments for end users through many applications from various industries. Many elements are needed to deliver the functionality of IoT. This includes device identification, sensing and collecting information, messaging, and information processing (Duan and Guo, 2021).

IoT architecture refers to the overall structure or framework of interconnected devices, networks, software, and systems that work together to enable the exchange of data and information between devices and applications. The IoT architecture consists of five main layers representing IoT systems' functionalities. These layers are the perception, network, middleware, application, and business layers. The perception layer consists of IoT physical devices. These devices collect information to deliver it to the network layer. The network layer delivers the information from the perception layer to the information processing system. The main task of this layer is to process the information received from the network layer and make decisions based on the results. The middleware layer refers to the software that connects and integrates various IoT devices, sensors, and applications within an IoT ecosystem. It serves as an intermediary layer, enabling communication, data management, and interoperability between the diverse components of IoT systems (Fersi et al., 2023). The application layer uses the processed information for global device management. Finally, the business layer controls the IoT system, applications, and services. In addition to these three layers, IoT architecture has other components, such as data storage, security, and management. These components ensure the safe and reliable operation of IoT systems (Hegde and Maddikunta, 2023). Overall, the architecture of IoT systems is designed to enable the seamless integration of different devices and technologies, providing real-time data and insights that can help improve efficiency, productivity, and decision-making in a variety of industries and sectors.

Figure 2 depicts the IoT Standards Reference Model with three horizontal services. Security is a vertical service applied across all the horizontal services and is one of the most important aspects to consider while making decisions about devices and Smart IoT Gateways. The Smart IoT Gateway collects data from devices and distributes it to the rest of the systems. The Full Stack IoT Platform indicates the source of the IoT data. Blockchain is evolving in the context of IoT, and organisations must plan the use of this function while deciding their IoT architecture (Anagnostopoulos et al., 2020).

Figure 2 IoT standards reference model (see online version for colours)



2.5 IoT security

Security plays a crucial role in the creation and implementation of IoT devices. If an IoT device is compromised due to an attack, it affects all connected sensors and actuators. In these situations, it is recommended to replace all affected sensors and hardware components. However, for real-time applications, replacing these compromised devices is impractical due to the extensive labour and high costs involved. It is challenging to develop a security architecture that can overcome this limitation using traditional methods such as access control, encryption, and user authentication (Gugueoth et al., 2023). Security risks in IoT can be widely classified into several types: access control issues, impersonation attacks, eavesdropping, as well as denial of service (DoS), and routing attacks. Security and privacy are considered the main challenges to adopting various IoT systems (Hasan et al., 2022). The growth of IoT devices creates new services and applications and several security vulnerabilities that become more apparent. Vendors of IoT devices need to consider security as a priority. Recently, the application domain of Blockchain has expanded to include the convergence of BCIoT networks. This coverage includes IoT device identification, authentication, sensor data storage, and secure data transfer. To ensure the proper security of networks within the IoT, it is imperative to maintain several fundamental properties: Confidentiality is paramount and can be reinforced through cryptographic protocols, which are integral in safeguarding network communications (Uddin et al., 2021). Blockchain technology enhances this aspect by equipping each IoT device with robust cryptographic capabilities, ensuring secure interactions among devices, and providing anonymity where necessary in IoT

applications. Integrity is essential to ensure that data transmitted by senders remains unaltered during its journey. This requires that IoT devices are designed in compliance with established standards that dictate the proper methods for data transmission, sharing, and collection. Availability is about ensuring consistent and uninterrupted service access. IoT services must remain accessible, reinforcing the network's reliability and user trust (Popoola et al., 2023; Uddin et al., 2021).

2.6 Blockchain-based IoT security

Past security vulnerabilities in IoT devices were often due to structural flaws in their design. Traditional IoT frameworks utilised a centralised architecture, where all data was consolidated in a single cloud repository. However, as the number of IoT devices continues to grow, there is an emerging need for decentralised security solutions, such as blockchain technology, to manage and safeguard data within IoT ecosystems. Given the decentralised nature of Blockchain, it can prevent a vulnerable device from transmitting false information and disrupting the network environment of a smart home, smart city, or intelligent factory. Blockchain uses the digital identity of the transactions using public key cryptography. This mechanism hides the real identity of IoT applications. The data of IoT applications are transported through infrastructure owned by multiple organisations. However, Blockchain's decentralised ledger provides more trust while moving data through infrastructure owned by multiple and diverse stakeholders. Blockchain networks provide smart contract facilities, allowing the creation of agreements to be executed when conditions are met (Gugueoth et al., 2023). An agreement on a standard protocol for data updates amongst all nodes must be established, and blocks should only be processed with the majority. This is called the consensus mechanism, which dictates the creation and addition of blocks to the ledger. Consensus mechanisms used in the current blockchain systems include PoW, PoS, PBFT, and DPoS (Tripathi et al., 2023). Smart contracts and Blockchains can be used to provide DDoS notifications across multiple domains (Sun et al., 2021). For example, filter blocklisted IP addresses between autonomous systems in public and distributed infrastructure. Furthermore, trusted Blockchain prevents attackers from directly installing malware on IoT devices. In addition, checking outgoing traffic prevents the spread of DDoS messages from IoT devices (Rodrigues et al., 2017).

The paper by Alajlan et al. (2023) thoroughly examined security concerns within blockchain systems, highlighting key issues like double-spending and 51% attacks. Double-Spending, where a user spends the same digital currency twice, undermines trust in the blockchain. To counteract this, the authors suggested consensus mechanisms and cryptographic methods. They also explored the threat of 51% attacks, where an attacker controls a majority of the network's computing power to manipulate the blockchain, proposing solutions like network partitioning. Additionally, the paper addressed the vulnerabilities of smart contracts, which automatically execute based on predefined conditions but are susceptible to code exploits and denial-of-service attacks, emphasising the need for robust security measures. According to Lohiya and Thakkar (2020), integrating Blockchain with IoT can be a solution regarding the security, reliability, and development of various IoT domains. Various applications and devices are often examined based on the data collected from the censors. Blockchain technology can significantly enhance IoT device security, as Hedge et al. (2023) describe. It strengthens protection by providing a decentralised model that mitigates the risk of single failure points and hacking, creates an unchangeable record of transactions to deter data

tampering, employs smart contracts to automate compliance with predefined rules, utilises cryptographic measures for data security and privacy, and establishes a decentralised identity framework to prevent unauthorised device impersonation and access. Collectively, these solutions create a more secure and reliable IoT environment. Combining BCIoT can provide a powerful security solution that enhances the security and privacy of IoT devices and data. However, it is essential to remember that implementing blockchain-based IoT security requires careful consideration of the specific use case and the potential trade-offs involved (Raj and Prakash, 2023; Banerjee et al., 2020).

3 Research methodology

This research uses a systematic literature review (SLR), which follows a process by which the author defines specific research questions and then use a particular methodology to collect and analyse relevant research to address the research questions (Yaqoop et al., 2019). In addition, this study follows the method suggested by Briner and Denyer (2012) in using PRISMA, which was introduced by Moher et al.'s (2009) research study. The author examines the title, abstract, and keywords. Given the immense volume of research, the author excluded all irrelevant journals from this study. Publishers such as ACM, IEEE, Sage, ScienceDirect, Elsevier, Springer, MDPI, Taylor and Francis, Google Scholar, and Wiley are used to extract research papers for further study. This section follows the inclusion and exclusion criteria guidelines to underscore relevant resources for this research study. The specific research strategy in this research involves the following steps:

This work contributes to the field by:

- Providing a comprehensive overview of both BCIoT architectures, establishing a foundation for understanding their potential integration.
- Reviewing existing blockchain solutions designed to address data security and management challenges within the IoT landscape. This analysis highlights current approaches and identifies areas for further development.
- Presenting an in-depth discussion on the integration of these solutions into practical IoT applications. This exploration goes beyond theoretical concepts and dives into real-world implementation considerations.
- Addressing the research questions formulated at the outset of this investigation. This ensures the work fulfils its intended purpose and provides valuable insights into the chosen area of study.

3.1 Research goals and questions

This research aims to analyse existing studies and their findings and provide answers to research questions created for this study. To address the research gap identified in the literature, the author developed three research questions, which are presented in Table 1.

Figure 3 The specific research strategy (see online version for colours)

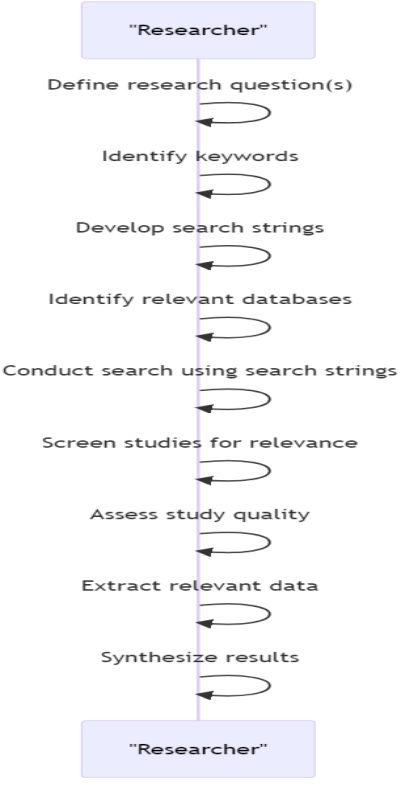


Table 1 Research questions

RQ#	*Research Question*	*Motivation*
1	What challenges do IoT applications face?	To identify and analyse studies related to the challenges encountered by IoT applications, shedding light on areas that need improvement or further research
2	How does Blockchain provide solutions in an IoT environment?	To explore and consolidate knowledge from various studies on the ways blockchain technology can address issues and enhance functionalities within IoT applications
3	Why do integrations between Blockchain and IoT applications encounter challenges?	To discuss, analyse, and conclude on the challenges that emerge when attempting to integrate blockchain technologies with IoT applications

3.2 Research protocol

The relevant research studies used for this research were identified by using specific keywords. The keywords were selected to provide answers to the research questions. The keywords focused on previous publications related to the research topic and questions. The operators were limited to AND and OR. The search strings were:

("blockchain" OR 'distributed ledger' OR "Peer-to-Peer") AND "security"

("blockchain" OR 'distributed ledger' OR 'Peer-to-Peer") AND ("cybersecurity' OR "information security")

Refined Blockchain and Security Focus with Exclusions:

("blockchain" OR 'distributed ledger' OR 'Peer-to-Peer") AND "security' NOT "cryptocurrency"

("blockchain" OR 'distributed ledger' OR 'Peer-to-Peer") AND ("cybersecurity' OR "security") NOT "bitcoin"

IoT-Specific Blockchain and Security:

("blockchain" AND 'IoT") AND ("cybersecurity' OR "security")

("blockchain" AND "Internet of Things") AND ("data protection" OR "privacy")

Advanced Search with Multiple Parameters:

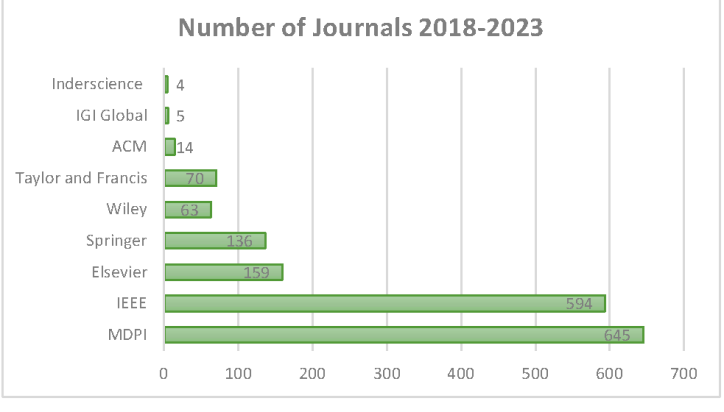
("blockchain" OR 'distributed ledger") AND ("IoT' OR "Internet of Things") AND ("security" OR 'cybersecurity' OR "data integrity")

("blockchain" AND 'IoT devices") AND ("encryption' OR "secure communication")

3.3 Inclusion and exclusion criteria

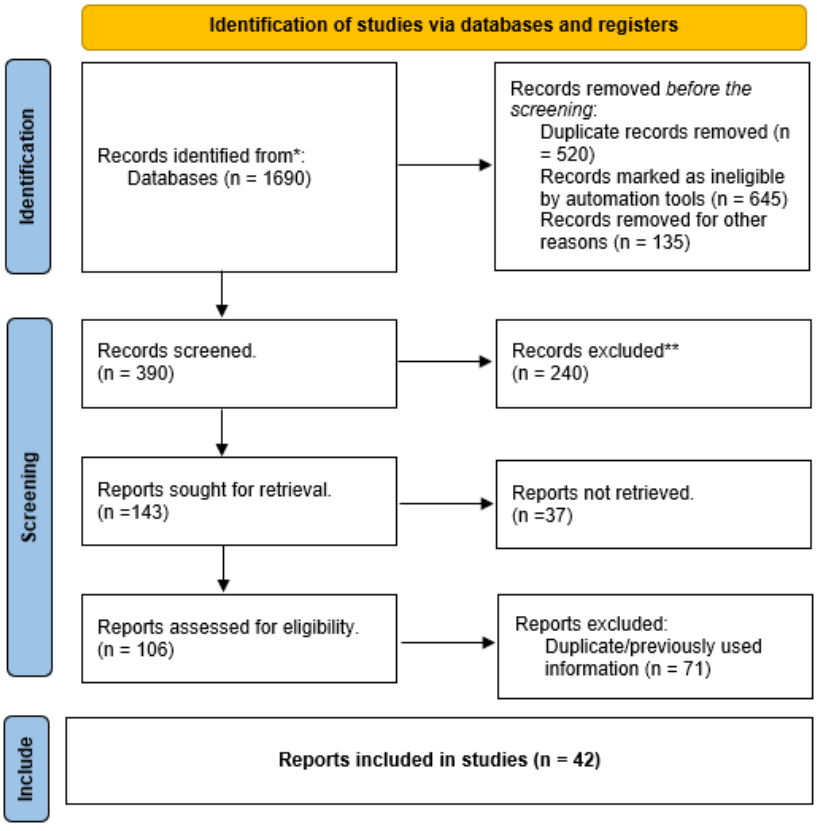
Database searches were conducted to find research papers from 2018 until 2023. The goal was to identify the distribution of journals and conference papers relevant to this study's central theme. Figure 4 lists the publishers and the range of years for the extracted papers. Based on the analysis, the results provided studies relevant to this study. The inclusion criteria reduced the papers to 49 valuable resources. The author of this paper used the abstract of all relevant results that align with the research goals, methodology, and findings. After completing the analysis of the abstracts, several papers were excluded. Duplicate and irrelevant studies were also excluded. The initial total number of papers retrieved was around 1690 studies.

Figure 4 Distribution of research papers (see online version for colours)



To identify relevant studies, a manual search was conducted through databases. As shown in Figure 5, this initial search yielded a set of studies. Applying the inclusion and exclusion criteria outlined by Moher et al. (2009), the number of studies for further analysis was reduced to 42. A PRISMA flowchart detailing the search process is presented in Figure 5.

Figure 5 Identification of studies via databases and registers (see online version for colours)



Following the above inclusion and exclusion criteria process, the 42 papers that were included in this research are listed in Table 2.

Table 2 Selected papers analysis

Year	*Authors*	*Reviewed topics*
2024	Tsai et al.	Smart Contracts
2024	Kharche et al.	IoT, Blockchain, Implementation
2023	Zhong et al.	Byzantine Fault-tolerant consensus algorithms
2023	Tripathi et al.	Blockchain, IoT, Security
2023	Popoola et al.	Security and Privacy, Smart Contracts
2023	Khashan and Khafajah	Blockchain-based Authentication
2023	Hussein et al.	Consensus Algorithm

Table 2 Selected papers analysis (continued)

Year	*Authors*	*Reviewed topics*
2023	Hemdan et al.	IoT-based blockchain challenges and integration
2023	Hegde and Maddikunta	Blockchain in Healthcare
2023	Raj and Prakash	Smart Contracts
2023	Fersi et al.	IoT Architecture
2023	Belen-Saglam et al.	GDPR and Public Blockchain
2023	Gugueoth et al.	IoT security
2023	Behera et al.	Blockchain, RFID
2023	Alghamdi et al.	Secure IoT, Blockchain security
2023	Albulayhi and Alsukayti	Blockchain, IoT Architecture
2023	Alajlan et al.	Blockchain Security
2023	Alam et al.	Blockchain, IoT, Security
2023	Adhikari and Ramkumar	IoT and Blockchain Challenges
2023	Chowdhury et al.	Blockchain and emerging issues
2023	Taloba et al.	Blockchain, Data Processing
2022	Tong et al.	Authentication Based on Blockchain for IoT
2022	Rahman et al.	Blockchain-Based IoT in Healthcare
2022	Prakash et al.	Blockchain threats and vulnerabilities
2022	Pawar and Palivela	Blockchain Framework
2022	Mishra and Pandia	IoT Attacks
2022	Gad et al.	Trends in Blockchain
2022	Chen et al.	Blockchain Cyberattacks
2022	Alzoubi	Blockchain in Healthcare
2021	Sun et al.	IoT-based HER system to realise privacy and traceability
2021	Uddin et al.	Blockchain in IoT
2020	Nguyen et al.	Blockchain and cloud of things
2020	Lohiya and Thakkar	IoT, data management
2020	Kumar and Tripathi	Data security, authentication, public key
2020	Kumar and Tripathi	Confidentiality, authentication, and integrity
2020	Ding et al.	IoT connectivity
2020	De Aguiar et al.	Blockchain, data management, and sharing
2020	Chenthara et al.	Cyber-attack-resistant BC-based HER framework
2020	Abdellatif et al.	IoT, edge computing
2020	Zhang et al.	Distributed storage, point-to-point transmission, consensus mechanism, Encryption algorithm, IoT
2020	Zhang et al.	IoT, storage, consensus mechanism, encryption
2020	Alrehaili and Mir	Blockchain-based Key Management

4 Research findings

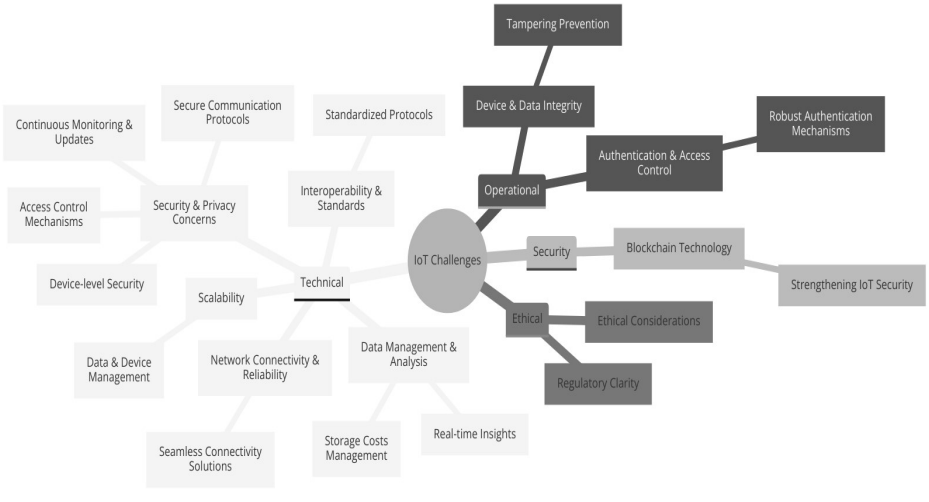
This section presents the answers to the research questions based on the literature mentioned discussed above.

***RQ1**. What challenges do IoT applications face?*

The deployment and operation of IoT applications are faced with numerous challenges that highlight the complexity of integrating these technologies into industrial processes and daily operations. These challenges span across several dimensions, including technical, operational, security, and physical aspects, each contributing to the landscape of IoT applications. A comprehensive security strategy that includes device-level security, secure communication protocols, access control mechanisms, and continuous monitoring and updates is required to address these challenges effectively. Adhering to industry best practices and standards is crucial for establishing a secure and resilient distributed IoT environment (Alghamdi et al., 2023). The diagram below outlines the multifaceted challenges in IoT applications, categorised into technical, operational, security, and ethical dimensions. It addresses technical issues like security, privacy, interoperability, scalability, data management, and connectivity. Operational concerns focus on device integrity and authentication, while security highlights the role of blockchain technology. Ethical considerations pertain to regulatory and ethical compliance in IoT implementations. Addressing these challenges requires technological advancements, regulatory clarity, and ethical considerations to advance the development of secure, efficient, and user-friendly IoT applications.

Figure 6 was developed based on the conclusions drawn from the literature and incorporates the contributions of various authors. Specifically, it presents summarised concepts that encompass the insights provided by Alghamdi et al. (2023), Mishra and Pandya (2021), Hegde and Maddikunta (2023), Mayer et al. (2021), and Tong et al. (2022), in response to research question one, depicted in a diagram created by the author of the journal.

Figure 6 IoT challenges



- *Security and privacy concerns*: The most critical challenge in IoT applications is ensuring the security and privacy of collected and processed data. IoT devices, capable of gathering large amounts of sensitive information, become prime targets for cyberattacks. Mishra and Pandya (2021) emphasise that the lack of encryption, outdated software, and unsecured services significantly compromise IoT device security. Furthermore, Hegde and Maddikunta (2023) highlight security and privacy as critical issues within the IoT domain, noting that standard security protocols are not universally applied, making IoT devices vulnerable to various attacks and leading to potentially massive losses.
- *Interoperability and standards*: The absence of standardised protocols severely limits the communication potential between devices from different ecosystems, hindering the realisation of comprehensive IoT solutions. This lack of interoperability is identified as a critical issue, underscoring the importance of industry-wide standards that facilitate seamless device interaction and integration (Kharche et al., 2024).
- *Scalability*: Efficiently scaling IoT networks to accommodate growing data volumes and device counts without compromising performance or reliability presents a significant challenge. The infrastructure must be capable of managing increased data and device demands, ensuring system quality and reliability are maintained.
- *Data management and analysis*: The management and analysis of the large datasets generated by IoT applications pose substantial challenges. Extracting meaningful insights in real-time and managing storage costs require effective data management strategies. This is compounded by the potential for data privacy risks when managed by centralised servers, as current IoT solutions often rely on cloud computing resources, leading to increased network latency (Mayer et al., 2021).
- *Network connectivity and reliability*: Achieving reliable network connectivity across various environments is crucial for the success of IoT applications. Challenges such as signal interference and bandwidth limitations require robust solutions that ensure seamless connectivity across different network types, including Wi-Fi, cellular, and Bluetooth (Mayer et al., 2021).
- *Device and data integrity*: Ensuring the integrity of IoT devices and their data is essential, particularly for applications involving critical infrastructure or sensitive information. Preventing tampering and unauthorised data alterations due to system errors is a significant concern that needs addressing to maintain trust in IoT applications.
- *Authentication and access control*: Strengthening security through reliable authentication and access control mechanisms is vital for verifying communicating parties and preventing the loss of confidential information. Liu et al. (2012) and Tong et al. (2022) stress the importance of robust authentication to safeguard against various network attacks, including eavesdropping, masquerading, and man-in-the-middle attacks.

In addressing the identified challenges, blockchain technology has a promising approach to strengthening IoT security. It presents viable solutions to reduce the sophisticated attacks and vulnerabilities prevalent in IoT devices. As IoT technology continues to advance, the strategies for navigating these challenges will evolve. This advancement is

set to facilitate the development of secure and efficient IoT systems, enabling their widespread deployment across various sectors.

***RQ2**. How does Blockchain provide benefits in an IoT environment?*

Blockchain technology emerges as a solution to the complex challenges encountered in the IoT environment, addressing critical concerns around security, privacy, data integrity, and interoperability. This section concludes the literature with insights into how blockchain technology contributes to resolving these issues, responding to the research question: How does Blockchain provide solutions in an IoT environment? Here is a detailed consideration of how Blockchain addresses these issues, supported by in-text references:

- *Establishing trust and ensuring data integrity*: Blockchain enables IoT devices to establish trust and verify data integrity through a secure, tamper-proof system. This capability allows for authenticating devices, establishing secure connections, and ensuring the integrity of data exchange without compromising security or privacy. Each transaction or data exchange within the IoT ecosystem is recorded across multiple nodes, ensuring no single entity can alter the data. Blockchain's role as a decentralised verifier ensures fault tolerance across the IoT ecosystem, crucially supporting data integrity and reliability (Wang et al., 2021). Blockchain's transparent nature allows all participants in the network to view transactions and data exchanges. This transparency, combined with the Blockchain's immutability, enhances participants' trust. Moreover, it enables easy auditing of data and transactions, providing a verifiable and secure record of all interactions within the IoT ecosystem. (Liu et al., 2023).
- *Combating security threats*: Blockchain technology is renowned for its immutable ledger, where once data is recorded, it cannot be altered or deleted. The immutability of Blockchain is critical in preventing attacks such as Man-in-the-middle, where deceptive information could be injected into the network, and DDoS attacks, which pose significant threats to IoT devices. Blockchain's distributed network structure enables IoT devices to share resources and bandwidth, effectively mitigating these risks (Valdovinos et al., 2021; Mann et al., 2020).
- *Enhancing authorisation with smart contracts*: Smart contracts on blockchain offer advanced authorisation techniques for IoT, automating contract execution once predefined conditions are met. Smart contracts can validate data from sensors before it is recorded on the Blockchain, ensuring that only accurate and verified data is stored. This feature streamlines operations and introduces higher security and efficiency in managing device interactions, functioning autonomously without centralised authority (Alzoubi, 2021; Dorri et al., 2017).
- *Ensuring privacy and security through encryption*: Blockchain employs consensus mechanisms like PoW, PoS, or others, depending on the Blockchain, to validate transactions. These mechanisms require network participants to agree on the validity of transactions before they are added to the Blockchain, further ensuring data integrity, and building trust among devices and users in the IoT ecosystem (Vaiyapuri et al., 2023). By utilising encryption and hashing, Blockchain enhances the security and privacy of IoT data. Public critical infrastructure further strengthens

this framework, ensuring secure communications and identity verification among parties and safeguarding data confidentiality and integrity.

- *Reducing costs and processing time*: Blockchain integration with IoT devices notably enhances operational efficiency and security, providing substantial cost benefits. By automating processes and reducing intermediaries, it lowers operational expenses. Enhanced security measures mitigate costs related to data breaches and fraud. Adopting energy-efficient consensus mechanisms, such as PoS, significantly reduces energy costs, which is crucial for energy-constrained IoT devices. Blockchain's decentralised nature also reduces maintenance costs associated with centralised storage, while its capacity for ensuring interoperability among diverse IoT technologies fosters long-term savings by simplifying technology integration. This streamlined approach reduces costs and shortens processing times for managing IoT networks, emphasising Blockchain's role in developing a more secure, efficient, and cost-effective IoT ecosystem. This efficiency is further supported by Blockchain's ability to optimise device maintenance and data transfer, enhancing the overall functionality of IoT systems (Taloba et al., 2023). Blockchain technology directly addresses IoT systems' core challenges, including security, privacy, interoperability, and data integrity issues. Through mechanisms like smart contracts, encryption, and its inherent decentralisation, Blockchain paves the way for the secure and efficient deployment of IoT applications across various sectors, as evidenced by the referenced studies.

The following process describes how Blockchain technology establishes a protected, decentralised, and effective system within an IoT framework. It attempts to address IoT networks' scalability, security, and data accuracy issues. The workflow of IoT blockchain is adaptable and can be tailored to different situations and data categories. This combination paves the way for automated and precise procedures in various sectors. Presented next is a prototype of the processing and communication workflow based on Blockchain for IoT. It encompasses the essential steps needed to achieve a secure and streamlined integration of IoT with Blockchain.

1 *IoT device collection*: An IoTDevice class represents a generic IoT device that collects data from its environment.

2 *Data processing*: The collected data is sent to an EdgeNode, which undergoes initial processing to prepare it for integration into the Blockchain network.

3 *Blockchain integration*: The BlockchainNetwork class adds processed data to the Blockchain, ensuring immutability and traceability.

4 *Smart contract automation*: SmartContract automates actions based on the processed data added to the Blockchain, facilitating automated decision-making.

5 *Secure data storage*: The DataStorage class securely stores blockchain data, maintaining data integrity and accessibility.

6 *User interaction*: A User class receives the results of the smart contract execution, enabling end-user interaction with the system.

7 *Access control*: The AccessControl class ensures system components and data are accessible only by authorised entities, enhancing system security.

8 *System monitoring*: A MonitoringSystem continuously monitors the data for abnormalities, generating alerts if necessary to maintain system integrity.

Table 3 presents summarised concepts that encompass the literature referenced in answering question 2, depicted as a simulation of the workflow by the journal author. It only summarises the process.

Table 3 Simulating the workflow

```
iot_device = IoTDevice ()
edge_node = EdgeNode ()
blockchain = BlockchainNetwork ()
smart_contract = SmartContract ()
data_storage = DataStorage ()
user = User ()
access_control = AccessControl ()
monitoring_system = MonitoringSystem ()

# Data Collection and Processing
data = iot_device.collect_data()
processed_data = edge_node.process_data (data)

# Blockchain Integration and Smart Contract Execution
block = Blockchain.add_to_ledger (processed_data)
result = smart_contract.execute (block)

# Data Storage and User Interaction
storage = data_storage.store_data (block)
user_response = user.receive_result(result)

# Security and Monitoring
secured_data = access_control.enforce_security ("IoT Data")
secured_blockchain = access_control.enforce_security ("Blockchain Netwc
system_status = monitoring_system.monitor (data)

# Conditional Alert Generation
if system_status != "system is normal":
    alert = "generate alert"
```

Blockchain technology directly addresses IoT systems' core challenges, including security, privacy, interoperability, and data integrity issues. Through mechanisms like smart contracts, encryption, and its inherent decentralisation, Blockchain paves the way for the secure and efficient deployment of IoT applications across various sectors, as evidenced by the referenced studies.

> ***RQ3***. *Why do integrations between Blockchain and IoT applications encounter challenges?*

Integrating Blockchain with the IoT offers numerous benefits, such as enhanced security, data integrity, and decentralised control, yet it introduces several challenges that need strategic solutions. Scalability emerges as a crucial issue, with blockchain platforms needing help to process the massive data volumes of IoT devices efficiently. The integration complexity, the necessity for advanced AI techniques for managing mining processes, and consensus mechanisms further complicate this landscape. Privacy concerns also show large, as blockchain transactions could inadvertently expose sensitive personal information. The expanding distributed ledger adds to the network complexity, escalating scalability and management challenges. Furthermore, cyber-attack vulnerabilities, including 51% attack and smart contract exploits, present serious security risks. Regulatory and compliance issues across different jurisdictions add another layer of complexity to blockchain operations within IoT contexts.

The transition from PoW to PoS offers a promising avenue for addressing these challenges, especially in IoT environments characterised by devices with limited computational resources, energy, and bandwidth. PoS's lower energy requirements make it an ideal choice for IoT systems, prioritising energy efficiency (Hussein et al., 2023). This mechanism not only conserves energy but also leverages the security and decentralised features of Blockchain to boost the reliability of IoT networks. Validators in a PoS system incentivised through staking play a crucial role in maintaining the integrity and security of the network, thereby mitigating potential fraud and ensuring data accuracy across devices. However, adopting PoS within IoT infrastructures requires careful consideration of its challenges, such as centralisation risks and specific security vulnerabilities. Effective strategies must be developed to ensure equitable validator selection, safeguard against IoT-specific security threats, and promote broad stakeholder participation. Below is a summary of the challenges encountered when considering the integration of BCIoT:

1 *Scalability*: Blockchain technology, primarily when implemented in traditional forms like Bitcoin or Ethereum, faces scalability issues due to the limited number of transactions it can process per second. On the other hand, IoT devices can generate massive volumes of data continuously, requiring a system that can handle high throughput efficiently.

2 *Resource constraints*: IoT devices often have limited computational power, storage capacity, and energy resources. Running complex blockchain operations on such devices, such as consensus algorithms, can be impractical due to these constraints.

3 *Network latency*: The decentralised nature of Blockchain can introduce latency in transaction processing and data verification, which might not be suitable for IoT applications requiring real-time or near-real-time data processing and decision-making.

4 *Security and privacy concerns*: While BCIoT technologies address security and privacy in their ways, integrating them raises complex issues. For instance, ensuring the privacy of sensitive IoT data when recorded on a public blockchain is a significant challenge.

5 *Interoperability*: There needs to be more standardisation across different IoT platforms and blockchain networks, making interoperability a significant hurdle. With standardised protocols, ensuring seamless communication and data exchange between diverse IoT devices and blockchain systems is more accessible.

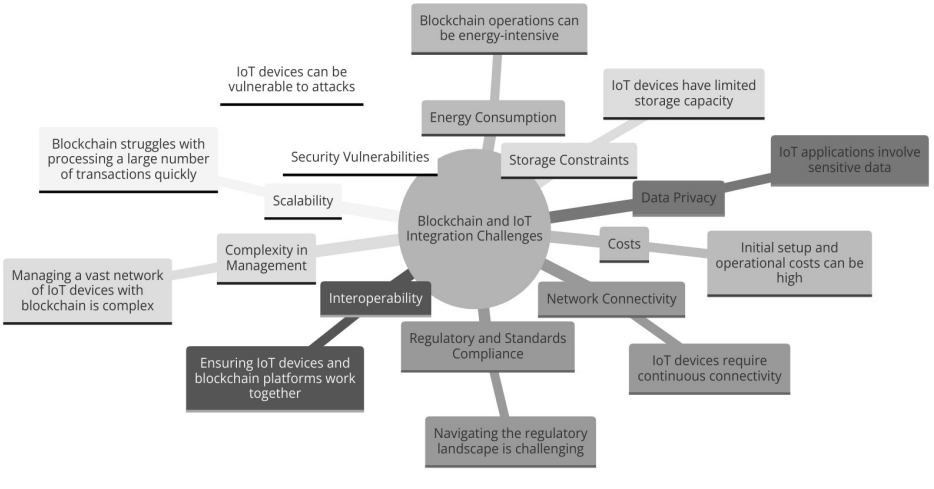
6 *Energy consumption*: The consensus mechanisms used in many blockchain networks, like PoW, are energy-intensive. This high energy consumption is due to the need for energy efficiency in IoT devices, especially those that are battery-powered or deployed in remote locations.

7 *Regulatory and legal issues*: Integrating BCIoT involves navigating complex regulatory and legal landscapes, varying significantly across jurisdictions. Compliance with data protection regulations, such as GDPR in Europe, becomes more complicated when IoT data is stored on a blockchain.

8 *Cost*: Implementing and maintaining a blockchain infrastructure can be costly, especially for large-scale IoT applications. The costs associated with transactions and data storage on the Blockchain must be economically viable for widespread adoption.

Addressing these issues demands focused research on developing scalable, secure, and privacy-preserving consensus mechanisms apt for IoT applications (Chen et al., 2022; Prakash et al., 2022; Shrivas et al., 2020). Alghamdi et al. (2023) highlighted the need for consensus algorithms that align with IoT's unique requirements, emphasising scalability, energy efficiency, interoperability, and compatibility with existing IoT protocols and standards, given the substantial computational resources, bandwidth, and delays associated with traditional blockchain networks. The future of BCIoT integration hinges on developing consensus protocols tailored to the distinctive challenges of IoT, including varied device standards, limited device memory, and managing large data volumes, ensuring an appropriate and efficient blockchain-IoT system. Figure 7 represents the various challenges encountered when considering BCIoT integration.

Figure 7 Blockchain and IoT integration challenges



5 Discussion

This paper examines the integration of Blockchain technology with the IoT, exploring both the potential benefits and the challenges of this convergence. Integrating Blockchain technology with the IoT represents a critical advancement in addressing the many challenges in the IoT landscape. As we explore this convergence, it becomes evident that combining these technologies offers significant benefits, particularly in enhancing the security, privacy, scalability, and interoperability of IoT systems. IoT applications are increasingly becoming integral to industrial processes and daily operations, yet they face substantial obstacles such as data privacy, security management, and interoperability issues. IoT system's decentralised and distributed nature increases these challenges, highlighting the critical need for robust security measures, including device authentication mechanisms like certificates or cryptographic keys, to ensure the trustworthiness of devices within distributed environments.

Blockchain technology emerges as a strategic solution, presenting advantages that bolster IoT systems' security and operational efficiency. Its decentralised, immutable, and transparent characteristics not only enhance security by eliminating single points of failure, thereby making networks more resilient to cyberattacks but also ensure data integrity through a tamper-proof record of transactions. The application of Blockchain extends to securing data transactions with advanced cryptographic algorithms, automating device authentication and authorisation through smart contracts, and fostering a trustless environment where trust is established via cryptographic verification, which is crucial for secure device-to-device communication.

To process the large number of transactions generated by IoT devices, blockchain platforms have adopted scalable consensus mechanisms, such as PoS or directed acyclic graphs (DAGs), which offer energy efficiency over traditional PoW systems. Furthermore, Blockchain facilitates interoperability across various IoT platforms, ensuring seamless communication and secure firmware/software updates, thereby safeguarding against potential threats.

Despite these advancements, the integration of BCIoT is challenging. Scalability issues, energy consumption, interoperability complexities, and regulatory compliance remain significant obstacles. The implementation of Blockchain introduces additional layers of complexity and usability issues, potentially impacting real-time data processing due to added latency. Moreover, while energy-efficient consensus mechanisms like PoS have been developed, the energy demands of blockchain operations, especially in large-scale IoT deployments, and the handling of massive data volumes generated by IoT devices demand innovative solutions. Regulatory compliance, particularly with laws focusing on data privacy such as the GDPR, poses another challenge given Blockchain's decentralised nature. Additionally, the lack of a standardised provider for blockchain interoperability hinders seamless integration across diverse ecosystems. It's also critical to acknowledge that Blockchain does not mitigate all security risks, with vulnerabilities in smart contract code and the physical security of IoT devices remaining relevant concerns.

The amalgamation of BCIoT holds immense promise in surmounting dominant challenges within IoT systems and enhancing security, efficiency, and scalability. Overcoming barriers related to scalability, interoperability, and energy consumption is vital in using the full potential of this integration. This effort is about technological innovation and about overlaying the way for a more secure, efficient, and interconnected digital future, requiring rigorous efforts from researchers, developers, and policymakers to realise its potential.

6 Conclusion

In this SLR based research, the author critically analyses and addresses various dimensions of IoT applications, blockchain technology, and the integration of both. Considering the first research question regarding the challenges IoT applications face, it was found that with the growing proliferation of IoT devices, ensuring security, interoperability, scalability, privacy, and reliability is paramount. The increased device connectivity exposes them to security breaches, data leaks, and cyber-attacks, requiring robust security protocols and efficient data handling mechanisms. Moving to the second research question on how Blockchain provides solutions in an IoT environment, it was identified that blockchain technology could enhance security, privacy, interoperability, and data integrity and automate processes using smart contracts. Blockchain's decentralised and tamper-proof nature ensures secure data sharing and storage, establishes device trust, and guarantees data integrity. However, its integration with IoT is challenging, as discussed in the third research question. Scalability issues, interoperability complexities, high energy consumption, and potential security vulnerabilities need careful consideration and practical solutions to leverage the potential of Blockchain in IoT applications fully. In conclusion, while IoT applications present numerous benefits in terms of connectivity and data availability, they also pose significant security, privacy, and reliability challenges. Blockchain technology offers a promising solution to these challenges, enhancing the security, privacy, and integrity of IoT applications. However, integrating BCIoT is not straightforward and presents its own challenges, including scalability, complexity, energy consumption, and potential security vulnerabilities. As we have followed the SLR method in this research, we have systematically gathered, reviewed, and synthesised existing literature to provide a comprehensive understanding of the current state of IoT and blockchain integration and identify areas requiring further research and development. The findings from this research provide organisations with valuable insights into integrating IoT and Blockchain, helping them navigate the complexities, mitigate risks, and leverage the technologies for enhanced security, efficiency, and innovation.

7 Future directions

Integrating Blockchain with IoT promises to enhance security and operational efficiency in IoT applications. Future research should concentrate on crafting scalable blockchain

solutions, ensuring they can support the expanding network of IoT devices while maintaining optimal performance. Additionally, exploring interoperable frameworks and standards is crucial for enabling smooth integration among various IoT devices and blockchain platforms. It is important to address the challenge posed by consensus algorithms, which currently demand high processing power, making them less suitable for IoT devices with limited computational capabilities. Developing lightweight consensus mechanisms that reduce processing demands will be vital in enabling the broader adoption of blockchain technology in IoT environments.

Conflicts of interest

The author(s) declare that there are no conflicts of interest regarding the publication of this paper.

Data availability

This research used secondary data: journal papers, conference papers, books, and reports in the reference section.

Acknowledgement

The comprehensive review of existing literature significantly enhanced the completion of this research. This process illuminated a wealth of information, providing a solid foundation and valuable insights that were instrumental in shaping the study. I extend my sincere gratitude to the authors and researchers whose works were consulted during this review. Their contributions have not only enriched my understanding but have also played a crucial role in guiding the direction and depth of this investigation.

References

Abdellatif, A.A., Al-Marridi, A.Z., Mohamed, A., Erbad, A., Chiasserini, C.F. and Refaey, A. (2020) 'Health: toward secure, blockchain-enabled healthcare systems', *IEEE Network*, Vol. 34, No. 4, pp.312–319, https://doi.org/10.1109/mnet.011.1900553

Adhikari, N. and Ramkumar, M. (2023) 'IoT and blockchain integration: applications, opportunities, and challenges', *Network*, Vol. 3, No. 1, pp.115–141, https://doi.org/10.3390/network3010006

Alajlan, R., Alhumam, N. and Frikha, M. (2023) 'Cybersecurity for blockchain-based IoT systems: a review', *Applied Sciences*, Vol. 13, No. 13, p.7432, https://doi.org/10.3390/app.13137432

Alam, S., Bhatia, S., Shuaib, M., Khubrani, M.M., Alfayez, F., Malibari, A.A. and Ahmad, S. (2023) 'An overview of blockchain and IoT integration for secure and reliable health records monitoring', *Sustainability*, Vol. 15, No. 7, p.5660, https://doi.org/10.3390/su15075660

Alam, T. (2022) 'Blockchain-based Internet of Things: review, current trends, applications, and future challenges', *Computers*, Vol. 12, No. 1, p.6, https://doi.org/10.3390/computers 12010006

Albulayhi, A.S. and Alsukayti, I.S. (2023) 'A blockchain-centric IoT architecture for effective smart contract-based management of IoT data communications', *Electronics*, Vol. 12, No. 12, p.2564, https://doi.org/10.3390/electronics12122564

Alghamdi, S., Albeshri, A. and Alhusayni, A. (2023) 'Enabling a secure IoT environment using a blockchain-based local-global consensus manager', *Electronics*, Vol. 12, No. 17, p.3721, https://doi.org/10.3390/electronics12173721

Alrehaili, A. and Mir, A. (2020) 'POSTER: blockchain-based key management protocol for resource-constrained IoT devices', *2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*, Riyadh, Saudi Arabia, pp.253–254, https://doi.org/ 10.1109/SMART-TECH49988.2020.00065

Alzoubi, M.M. (2021) 'Blockchain technology solutions in healthcare: a systematic review', *International Journal of Blockchains and Cryptocurrencies*, Vol. 2, No. 3, pp.205–221, https://doi.org/10.1504/Ijbc.2021.119881

Anagnostopoulos, N.A., Ahmad, S., Arul, T., Steinmetzer, D., Hollick, M. and Katzenbeisser, S. (2020) 'Low-cost security for next-generation IoT networks', *ACM Transactions on Internet Technology*, Vol. 20, No. 3, pp.1–31, https://doi.org/10.1145/3406280

Banerjee, A., Biswas, K. and Chattopadhyay, A. (2020) 'Blockchain-based IoT security: a systematic review', *Journal of Ambient Intelligence and Humanized Computing*, Vol. 11, No. 3, pp.1217–1246.

Behera, T.K., Panda, B.S. and Samanta, D. (2023) 'How blockchain solves the supply chain problems using RFID techniques', *International Journal of Blockchains and Cryptocurrencies*, Vol. 4, No. 2, pp.105–122, https://doi.org/10.1504/IJBC.2023.132701

Belen-Saglam, R., Altuncu, E., Lü, Y. and Li, S. (2023) 'A systematic literature review of the tension between the GDPR and public blockchain systems', *Blockchain: Research and Applications*, Vol. 4, No. 2, p.100129, https://doi.org/10.1016/j.bcra.2023.100129

Briner, R.B. and Denyer, D. (2012) *Systematic Review and Evidence Synthesis as a Practice and Scholarship Tool*, Oxford University Press eBooks, pp.112–129, https://doi.org/ 10.1093/oxfordhb/9780199763986.013.0007

Cecilia Eberendu, A. and Ifeanyi Chinebu, T. (2021) 'Can blockchain be a solution to IoT technical and security issues?', *International Journal of Network Security and Its Applications*, Vol. 13, No. 6, pp.123–132, https://doi.org/10.5121/ijnsa.2021.13609

Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M. and Cai, Z. (2022) 'A survey on blockchain systems: attacks, defenses, and privacy preservation', *High-Confidence Computing*, Vol. 2, No. 2, p.100048, https://doi.org/10.1016/j.hcc.2021.100048

Chenthara, S., Ahmed, K., Wang, H., Whittaker, F. and Chen, Z. (2020) 'Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology', *PLOS ONE*, Vol. 15, No. 12, p.e0243043, https://doi.org/10.1371/journal.pone.0243043

Chowdhury, E., Stasi, A. and Pellegrino, A. (2023) 'Blockchain technology in financial accounting: emerging regulatory issues', *Review of Financial Economics*, Vol. 21, pp.862–868.

De Aguiar, E.J., Faiçal, B.S., Krishnamachari, B. and Ueyama, J. (2021) 'A survey of blockchain-based strategies for healthcare', *ACM Computing Surveys*, Vol. 53, No. 2, pp.1–27, https://doi.org/10.1145/3376915

Ding, J., Nemati, M., Ranaweera, C. and Choi, J. (2020) 'IoT connectivity technologies and applications: a survey', *IEEE Access*, Vol. 8, pp.67646–67673, https://doi.org/10.1109/access.2020.2985932

Dorri, A., Kanhere, S.S. and Jurdak, R. (2017) 'Towards an optimized blockchain for IoT', *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, April, Pittsburgh, PA, USA, pp.173–178, https://doi.org/10.1145/3054977.3055003

Duan, R. and Li, G. (2021) 'Application of Blockchain for Internet of Things: a bibliometric analysis', *Mathematical Problems in Engineering*, Vol. 2021, pp.1–16, https://doi.org/10.1155/2021/5547530

ElGayyar, M.M., ElYamany, H.F., Grolinger, K., Capretz, M.A. and Mir, S. (2020) 'Blockchain-based federated identity and auditing', *International Journal of Blockchains and Cryptocurrencies*, Vol. 1, No. 2, pp.179–205, doi: 10.1504/IJBC.2020.109004.

Fersi, G., Ben Hammouda, A. and Derbel, F. (2023) 'Chord-based distributed middleware architecture for the Internet of Things', *2023 International Wireless Communications and Mobile Computing* (*IWCMC*), Marrakesh, Morocco, pp.812–817, https://doi.org/10.1109/IWCMC58020.2023.10182923

Gad, A.G., Mosa, D.T., Abualigah, L. and Abohany, A.A. (2022) 'Emerging trends in blockchain technology and applications: a review and outlook', *Journal of King Saud University-Computer and Information Sciences*, Vol. 34, No. 9, pp.6719–6742, https://doi.org/10.1016/j.jksuci.2022.03.007

Gu, A., Yin, Z., Cui, C. and Li, Y. (2020) 'Integrated functional safety and security diagnosis mechanism of CPS based on blockchain', *IEEE Access*, Vol. 8, pp.15241–15255, https://doi.org/10.1109/ACCESS.2020.2967453

Gugueoth, V., Safavat, S. and Shetty, S. (2023) 'Security of Internet of Things (IoT) using federated learning and deep learning – recent advancements, issues and prospects', *ICT Express*, Vol. 9, No. 5, pp.941–960, https://doi.org/10.1016/j.icte.2023.03.006

Hasan, H.R., Salah, K., Yaqoob, I., Jayaraman, R., Pesic, S. and Omar, M. (2022) 'Trustworthy IoT data streaming using blockchain and IPFS', *IEEE Access*, Vol. 10, pp.17707–17721, doi: 10.1109/ACCESS.2022.3149312.

Hegde, P. and Maddikunta, P.K.R. (2023) 'Amalgamation of blockchain with resource-constrained IoT devices for healthcare applications–state of art, challenges and future directions', *International Journal of Cognitive Computing in Engineering*, https://doi.org/10.1016/j.ijcce.2023.06.002

Hemdan, E.E., El-Shafai, W. and Sayed, A. (2023) 'Integrating digital twins with IoT-based blockchain: concept, architecture, challenges, and future scope', *Wireless Personal Communications*, Vol. 131, No. 3, pp.2193–2216, https://doi.org/10.1007/s11277-023-10538-6

Hussein, Z., Salama, M.A. and El-Rahman, S.A. (2023) 'Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms', *Cybersecurity*, Vol. 6, No. 1, p.30, https://doi.org/10.1186/s42400-023-00163-y

Kharche, A., Badholia, S. and Upadhyay, R.K. (2024) 'Implementation of blockchain technology in integrated IoT networks for constructing scalable ITS systems in India', *Blockchain: Research and Applications*, p.100188, https://doi.org/10.1016/j.bcra.2024.100188

Khashan, O.A. and Khafajah, N.M. (2023) 'Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems', *Journal of King Saud University-Computer and Information Sciences*, Vol. 35, No. 2, pp.726–739, https://doi.org/10.1016/j.jksuci.2023.01.011

Liu, J., Xiao, Y. and Chen, C.L.P. (2012) 'Authentication and access control in the Internet of Things', *2012 32nd International Conference on Distributed Computing Systems Workshops*, Macau, China, pp.588–592, https://doi.org/10.1109/ICDCSW.2012.23

Liu, Y., Wang, J., Yan, Z., Wan, Z. and Jäntti, R. (2023) 'A survey on blockchain-based trust management for Internet of Things', *IEEE Internet of Things Journal*, Vol. 10, No. 7, pp.5898–5922, doi: 10.1109/JIoT.2023.3237893.

Lohiya, R. and Thakkar, A. (2020) 'Application domains, evaluation data sets, and research challenges of IoT: a systematic review', *IEEE Internet of Things Journal*, Vol. 8, No. 11, pp.8774–8798, doi: 10.1109/JIOT.2020.3048439.

Lu, Y. (2019) 'The blockchain: state-of-the-art and research challenges', *Journal of Industrial Information Integration*, Vol. 15, pp.80–90, https://doi.org/10.1016/j.jii.2019.04.002

Mann, P., Tyagi, N., Gautam, S. and Rana, A. (2020) 'Classification of various types of attacks in IoT environment', *2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)*, pp.346–350, Bhimtal, India, https://doi.org/10.1109/CICN49253.2020.9242592

Mayer, A.H., Rodrigues, V.F., da Costa, C.A., da Rosa Righi, R., Roehrs, A. and Antunes, R.S. (2021) 'Fogchain: A fog computing architecture integrating blockchain and the Internet of Things for personal health records', *IEEE Access*, Vol. 9, pp.122723–122737, doi: 10.1109/ACCESS.2021.3109822.

Mishra, N. and Pandya, S. (2021) 'Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review', *IEEE Access*, Vol. 9, pp.59353–59377, https://doi.org/10.1109/access.2021.3073408

Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G. and The PRISMA Group (2009) 'Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement', *PLoS Med.*, Vol. 6, No. 7, p.e1000097, DOI: 10.1371/journal.pmed1000097.

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*, Retrieved 30 July, 2023, from https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Goldfeder, S. (2016) *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, Princeton, NJ, USA, https://bitcoinbook.cs.princeton.edu/

Nguyen, D.C., Pathirana, P.N., Ding, M. and Seneviratne, A. (2020) 'Integration of blockchain and cloud of things: architecture, applications and challenges', *IEEE Communications Surveys and Tutorials*, Vol. 22, No. 4, pp.2521–2549, https://doi.org/10.1109/comst.2020.3020092

Pawar, S. and Palivela, D.H. (2022) 'LCCI: a framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)', *International Journal of Information Management Data Insights*, Vol. 2, No. 1, p.100080, https://doi.org/10.1016/j.jjimei.2022.100080

Popoola, O.J., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehia, A. and Popoola, J. (2023) 'A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions', *Blockchain: Research and Applications*, p.100178, https://doi.org/10.1016/j.bcra.2023.100178

Prakash, R., Anoop, V. and Asharaf, S. (2022) 'Blockchain technology for cybersecurity: a text mining literature analysis', *International Journal of Information Management Data Insights*, Vol. 2, No. 2, p.100112, https://doi.org/10.1016/j.jjimei.2022.100112

Rahman, M.S., Islam, M.A., Uddin, M.A. and Stea, G. (2022) 'A survey of blockchain-based IoT eHealthcare: Applications, research issues, and challenges', *Internet of Things*, Vol. 19, p.100551, https://doi.org/10.1016/j.IoT.2022.100551

Raj, A. and Prakash, S. (2023) 'Smart contract-based secure decentralized smart healthcare system', *International Journal of Software Innovation (IJSI)*, Vol. 11, No. 1, pp.1–20, doi: 10.4018/ijsi.315742.

Rodrigues, B., Bocek, T., Lareida, A., Hausheer, D., Rafati, S. and Stiller, B. (2017) 'A blockchain-based architecture for collaborative DDoS mitigation with smart contracts', *Security of Networks and Services in an All-Connected World: 11th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2017*, Zurich, Switzerland, 10–13 July, 2017, Proceedings 11, Springer International Publishing, pp.16–29, https://doi.org/10.1007/978-3-319-60774-0_2

Shrivas, M.K., Dean, T.Y. and Brunda, S.S. (2020) 'The disruptive blockchain security threats and threat categorization', *2020 First International Conference on Power, Control and Computing Technologies (ICPC2T)*, Raipur, India, https://doi.org/10.1109/icpc2t48082.2020.9071475

Sun, B., Zhihui, L. and Li, Q. (2021) 'Obstetrics nursing and medical health system based on blockchain technology', *Journal of Healthcare Engineering*, Vol. 2021, pp.1–11, https://doi.org/10.1155/2021/6631457

Sun, Y., Yan, B., Yao, Y. and Yu, J. (2021) 'DT-DPoS: a delegated proof of stake consensus algorithm with dynamic trust', *Procedia Computer Science*, Vol. 187, pp.371–376, https://doi.org/10.1016/j.procs.2021.04.113

Taloba, A.I., Elhadad, A., Rayan, A., Abd El-Aziz, R.M., Salem, M., Alzahrani, A.A., and Park, C. (2023) 'A blockchain-based hybrid platform for multimedia data processing in IoT healthcare', *Alexandria Engineering Journal*, Vol. 65, pp.263–274, https://doi.org/10.1016/j.aej.2022.09.031

Tong, F., Chen, X., Wang, K. and Zhang, Y. (2022) 'CCAP: a complete cross-domain authentication based on blockchain for internet of things', *IEEE Transactions on Information Forensics and Security*, Vol. 17, pp.3789–3800, https://doi.org/10.1109/tifs.2022.3214733

Tripathi, G., Ahad, M.A. and Casalino, G. (2023) 'A comprehensive review of blockchain technology: underlying principles and historical background with future challenges', *Decision Analytics Journal*, Vol. 9, p.100344, https://doi.org/10.1016/j.dajour.2023.100344

Tsai, W.C. and Shen, C.W. (2024) 'Using a smart contract for the floral supply chain', *Asia Pacific Management Review*, https://doi.org/10.1016/j.apmrv.2023.12.004

Uddin, M.A., Stranieri, A., Gondal, I. and Balasubramanian, V. (2021) 'A survey on the adoption of blockchain in IoT: challenges and solutions', *Blockchain: Research and Applications*, Vol. 2, No. 2, p.100006, https://doi.org/10.1016/j.bcra.2021.100006

Vaiyapuri, T., Shankar, K., Rajendran, S., Kumar, S., Acharya, S. and Kim, H. (2023) 'Blockchain assisted data edge verification with consensus algorithm for machine learning assisted IoT', *IEEE Access*, Vol. 11, pp.55370–55379, https://doi.org/10.1109/ACCESS.2023.3280798

Valdovinos, I.A., Pérez-díaz, J.A., Choo, K.K.R. and Botero, J.F. (2021) 'Emerging DDoS attack detection and mitigation strategies in software-defined networks: taxonomy, challenges, and future directions', *Journal of Network and Computer Applications*, Vol. 187, p.103093.

Wang, H., Zhang, Y., Xu, K. and Xu, L. (2021) 'Blockchain-based IoT security: a comprehensive survey', *IEEE Communications Surveys and Tutorials*, Vol. 23, No. 2, pp.1431–1462.

Yaga, D., Mell, P., Roby, N. and Scarfone, K. (2019) *Blockchain Technology Overview*, National Institute of Standards and Technology Internal Report 8202, https://doi.org/10.6028/NIST.IR.8202

Yang, X., Zhang, Y. and Li, X. (2020) 'A survey of blockchain technology for IoT: applications, challenges, and opportunities', *Future Generation Computer Systems*, Vol. 108, pp.441–459.

Zhang, H., Lang, W., Liu, C. and Zhang, B. (2020) 'A blockchain-based security approach architecture for the Internet of Things', *2020 IEEE 4th Information Technology, Networking, Electronic, and Automation Control Conference (ITNEC)*, Chongqing, China, https://doi.org/10.1109/itnec48623.

Zhang, Y., Zhang, J., Zhao, Q., Zhang, H. and Zhu, X. (2021) 'Blockchain-based framework for smart manufacturing in IoT environment', *IEEE Internet of Things Journal*, Vol. 8, No. 3, pp.1633–1643.

Zhong, W., Yang, C., Liang, W., Cai, J., Chen, L., Liao, J. and Xiong, N. (2023) 'Byzantine fault-tolerant consensus algorithms: a survey', *Electronics*, Vol. 12, No. 18, p.3801, https://doi.org/10.3390/electronics12183801