Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Review:

Convergence of blockchain and Internet of Things: integration, security, and use cases

Robertas DAMAŠEVIČIUS[1], Sanjay MISRA[2], Rytis MASKELIŪNAS[3], Anand NAYYAR[‡4]

[1]*Department of Applied Informatics, Vytautas Magnus University, Kaunas 44404, Lithuania*
[2]*Department of Applied Data Science, Institute for Energy Technology, Halden 1777, Norway*
[3]*Department of Multimedia Engineering, Kaunas University of Technology, Kaunas 51368, Lithuania*
[4]*Graduate School, Faculty of Information Technology, Duy Tan University, Da Nang 550000, Viet Nam*
E-mail: robertas.damasevicius@vdu.lt; sanjay.misra@ife.no; rytis.maskeliunas@ktu.lt; anandnayyar@duytan.edu.vn
Received Mar. 28, 2023; Revision accepted June 9, 2023; Crosschecked Aug. 6, 2024

Abstract: Internet of Things (IoT) devices are becoming increasingly ubiquitous, and their adoption is growing at an exponential rate. However, they are vulnerable to security breaches, and traditional security mechanisms are not enough to protect them. The massive amounts of data generated by IoT devices can be easily manipulated or stolen, posing significant privacy concerns. This paper is to provide a comprehensive overview of the integration of blockchain and IoT technologies and their potential to enhance the security and privacy of IoT systems. The paper examines various security issues and vulnerabilities in IoT and explores how blockchain-based solutions can be used to address them. It provides insights into the various security issues and vulnerabilities in IoT and explores how blockchain can be used to enhance security and privacy. The paper also discusses the potential applications of blockchain-based IoT (B-IoT) systems in various sectors, such as healthcare, transportation, and supply chain management. The paper reveals that the integration of blockchain and IoT has the potential to enhance the security, privacy, and trustworthiness of IoT systems. The multi-layered architecture of B-IoT, consisting of perception, network, data processing, and application layers, provides a comprehensive framework for the integration of blockchain and IoT technologies. The study identifies various security solutions for B-IoT, including smart contracts, decentralized control, immutable data storage, identity and access management (IAM), and consensus mechanisms. The study also discusses the challenges and future research directions in the field of B-IoT.

Key words: Blockchain; Internet of Things (IoT); Blockchain-based IoT (B-IoT); Security; Scalability; Privacy
https://doi.org/10.1631/FITEE.2300215 **CLC number:** TP309

1 Introduction

The emergence of Internet of Things (IoT) has created a surge in the number of interconnected devices, leading to an exponential increase in the amount of data generated. The need for secure and decentralized management of data has given rise to the use of blockchain technology. Blockchain technology is recognized as a promising solution to address the challenges of secure, decentralized, and tamper-proof data storage and management (Fernández-Caramés and Fraga-Lamas, 2018; Wang X et al., 2019b). In recent years, the convergence of blockchain and IoT has gained significant attention, giving rise to the concept of blockchain-based Internet of Things (B-IoT) (Alam T, 2023). The integration of blockchain and IoT creates a distributed, secure, and decentralized network of connected devices, enabling secure and reliable communication between devices and data sharing among multiple parties (Abed et al., 2023). B-IoT is expected

‡ Corresponding author
ORCID: Robertas DAMAŠEVIČIUS, https://orcid.org/0000-0001-9990-1084; Anand NAYYAR, https://orcid.org/0000-0002-9821-6146

to play a crucial role in various application domains, including healthcare, supply chain management, energy, transportation, and smart cities. The potential benefits of B-IoT include enhanced security, privacy, transparency, and efficiency in data management, making it a promising technology for future research and development.

B-IoT combines two important technologies: blockchain and IoT. Blockchain is a distributed ledger technology that provides a secure and transparent way to store and exchange data without the need for a trusted intermediary (Zheng et al., 2017). The IoT refers to a network of interconnected devices that collect and exchange data over the Internet (Gubbi et al., 2013). In the context of B-IoT, these devices can include sensors, smart meters, and other IoT devices. B-IoT can be defined as a decentralized and secure system that combines the benefits of blockchain and IoT to create a transparent and tamper-proof environment for data exchange and storage. The main concepts in B-IoT include smart contracts, decentralized control, consensus mechanisms, immutable data storage, identity and access management (IAM), and multi-layered architecture. Smart contracts are self-executing contracts with the terms of agreement between buyers and sellers being directly written into lines of code (Zheng et al., 2020). Decentralized control refers to the absence of a single central authority in control of a system, with control instead being distributed among multiple nodes (Griffin et al., 2021). Consensus mechanisms refer to the process by which multiple nodes in a network agree on a single version of the truth. Immutable data storage refers to the practice of storing data in a way that prevents them from being altered or deleted (Wang WB et al., 2019). IAM involves the secure management of user identities and their access to resources (Ren et al., 2019). Finally, multi-layered architecture refers to the practice of organizing a system into multiple layers to improve its security, scalability, and manageability.

B-IoT is an emerging technology that combines the security features of blockchain with the data management capabilities of IoT to create a secure, decentralized, and tamper-proof data management system (Viriyasitavat et al., 2019; El-Masri and Hussain, 2021). The combination of blockchain and IoT is expected to transform various industries (Gill et al., 2019; Wang X et al., 2019a), including healthcare (Bigini et al., 2020; Ratta et al., 2021; Rahman et al., 2022), agriculture (Torky and Hassanein, 2020), manufacturing (Alkhateeb et al., 2022; Kumar RL et al., 2022), environmental monitoring (Bhattacharya et al., 2022), construction (Elghaish et al., 2021; Xiong et al., 2022), energy management (Li J et al., 2023), smart cities (Chen et al., 2020; Alam T, 2022), forensics (Akinbi et al., 2022), autonomous vehicles (Biswas and Wang, 2023), and transportation (Sunny et al., 2022).

B-IoT is expected to bring several advantages compared to traditional IoT systems. One of the key benefits of B-IoT is enhanced security and privacy. Blockchain technology provides a tamper-proof and immutable ledger that can help prevent unauthorized access and tampering with data, and ensure the integrity of the data collected by IoT devices. B-IoT also offers increased transparency and accountability, because each transaction recorded on the blockchain can be traced back to its origin, making it easier to identify any malicious or fraudulent activity. Another advantage of B-IoT is increased efficiency and reduced costs as blockchain-based smart contracts can automate various processes, such as payments, data sharing, and decision-making, eliminating the need for intermediaries and reducing transaction fees. B-IoT can also improve data interoperability and integration by enabling seamless data sharing and collaboration among different entities, leading to better decision-making and improved services. Overall, B-IoT technology has the potential to revolutionize various industries by providing secure, transparent, and efficient systems for managing IoT data and devices. Despite the enormous potential of B-IoT, there are several challenges that need to be addressed. The scalability and security of B-IoT are the primary concerns that must be addressed. The scalability challenge arises due to the increasing number of IoT devices and the need for faster and more efficient data management (Rahman et al., 2022). The security challenge arises due to the potential vulnerabilities of IoT devices and the need for a robust security mechanism to protect the data from unauthorized access (Bagga et al., 2022).

The integration of blockchain technology with the IoT has emerged as a powerful paradigm with tremendous potential to revolutionize various industries and enhance the security, transparency, and efficiency

of IoT systems. However, several challenges and research gaps still exist in effectively harnessing the benefits of blockchain in the context of IoT. This paper aims to address these challenges and provide valuable insights into the design, implementation, and optimization of B-IoT solutions. By exploring novel approaches, algorithms, and architectures, this research seeks to contribute to the advancement of blockchain technology and its integration with the IoT, ultimately paving the way for more secure and trustworthy IoT applications across various domains. The motivation behind this paper is to provide researchers, practitioners, and industry professionals with a comprehensive understanding of the potential and limitations of B-IoT systems and to inspire further research and development in this exciting and evolving field.

The purpose of this work is to provide a comprehensive review of the integration of blockchain and IoT technologies, their security solutions, and their applications in various fields. By examining the current state of the research field and analyzing key publications, this study aims to highlight the potential benefits and challenges of B-IoT. The significance of this work lies in its contribution to the understanding of how blockchain and IoT can be combined to create secure, decentralized, and tamper-proof systems for data management and communication. This research provides insights into the potential impact of B-IoT in industries such as healthcare, supply chain management, energy, transportation, and smart cities. By identifying the challenges and future research directions, this study serves as a guide for researchers, practitioners, and policymakers in exploring the possibilities and implications of B-IoT technology.

This research addresses the major puzzle and controversy around the integration of blockchain and IoT technologies. Although the potential benefits of this integration are widely recognized, there are significant challenges and unresolved issues that need to be addressed. The puzzle lies in finding effective solutions to ensure the seamless integration, scalability, security, and privacy of B-IoT systems. The controversy arises from the divergent opinions and approaches in tackling these challenges, as well as the ongoing debate on the feasibility and practicality of implementing blockchain in IoT applications. By addressing these puzzles and controversies, this research aims to provide valuable insights and recommendations to bridge the gap between theory and practice in B-IoT systems.

This paper is structured in several sections starting with an introduction, followed by a literature review of blockchain technology, IoT, and their integration in Section 2. Section 3 discusses the B-IoT layers, and the security issues and vulnerabilities in B-IoT, including threats, attacks, and countermeasures. Section 4 discusses the blockchain-based security solutions in IoT and their various components, such as smart contracts, immutable data storage, consensus mechanisms, and IAM. Section 5 discusses the use cases and applications of B-IoT in different sectors, including smart cities, transportation, energy and utilities, healthcare, and supply chain management. Section 6 analyzes the challenges and limitations of B-IoT, including scalability, security vulnerabilities, and convergence challenges. Section 7 addresses the ethical and social issues of B-IoT. Section 8 addresses the limitations and future research directions. Finally, concluding remarks are given in Section 9.

2 Overview of IoT and blockchain

2.1 Concept and features of IoT

IoT refers to a network of interconnected physical objects, such as devices, sensors, vehicles, and buildings, which can collect and share data with each other or with other systems over the Internet (Yunana et al., 2021). These objects can range from simple devices like home appliances and wearables to complex systems like smart cities and industrial machines. The main goal of IoT is to enable seamless communication and coordination between physical objects and digital systems, thereby improving efficiency, productivity, and quality of life.

An IoT architecture (Fig. 1) typically includes devices or things, gateways, network infrastructure, cloud platforms, and applications. IoT devices or things are the physical objects such as sensors, actuators, and smart devices that collect and transmit data. Gateways act as intermediaries between devices and the cloud, and perform data aggregation, filtering, and protocol translation. Network infrastructure includes wired and wireless networks that provide connectivity between devices, gateways, and the cloud. Cloud platforms

provide data storage, virtual machines, processing, and analytics capabilities, which allow applications to access and analyze the data generated by devices, while cloud federations provide increased resilience and enhanced performance, and prevent vendor lock-in (Doyle et al., 2022). Finally, applications are the user-facing interfaces that allow users to interact with the system and make use of the data generated by devices.

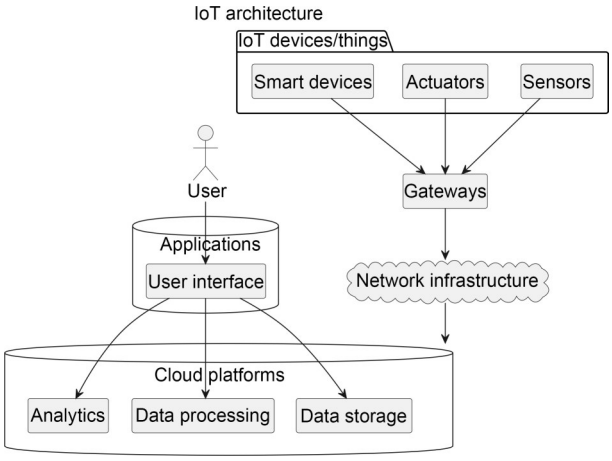

Fig. 1 Generic architecture of Internet of Things (IoT)

One of the key features of IoT is its ability to generate large amounts of data from a wide range of sources, including sensors, cameras, and other devices. These data can be used for a variety of purposes, such as real-time monitoring, predictive analytics, and automation. Another key feature of IoT is its ability to provide remote access and control of physical objects, allowing users to manage and interact with their environments from anywhere. IoT has the potential to enable new business models and revenue streams, as well as new applications and services that were not previously possible (Bublitz et al., 2019). For example, IoT can be used to create new products and services that leverage the data and insights generated by connected devices, such as personalized healthcare, predictive maintenance, and smart energy management. Despite its many benefits, IoT poses significant challenges in terms of security, privacy, and interoperability (Čolaković and Hadžialić, 2018). As more and more devices are connected to the Internet, the risk of cyberattacks and data breaches increases, and the complexity of managing and securing these devices becomes higher. Moreover, the lack of standardization and interoperability among different IoT devices and systems can hinder their adoption and scalability.

2.2 Concept and emergence of blockchain

Blockchain is a distributed ledger technology that provides a secure and decentralized platform for recording and sharing data. It was first introduced in 2008 as part of a white paper authored by an unknown person or group going by the pseudonym Satoshi Nakamoto, which outlined the concept of a digital currency called Bitcoin. Blockchain was initially used as the underlying technology for Bitcoin to provide secure and transparent transactions between users without the need for a centralized intermediary such as a bank.

Blockchain technology is built on a network of computers, called nodes, that work together to maintain a shared database of transactions (Zhao, 2019). A blockchain system is composed of multiple components, including nodes, blocks, transactions, consensus algorithms, and network protocols (Fig. 2). Nodes are the computing devices that participate in the blockchain network and store copies of the distributed ledger. Each node in the network stores a copy of the entire database, and every transaction that takes place on the network is recorded in a block, which is added to the chain of existing blocks in a permanent and unalterable way. This makes the data stored on the blockchain transparent, secure, and resistant to tampering or hacking attempts. Nodes are further divided into two types: full nodes and light nodes. Full nodes maintain a complete copy of the blockchain and participate in the validation and consensus processes, whereas light nodes store only a subset of the blockchain and rely on full nodes for validation and consensus.

Transactions are the data entries that contain information about the exchange of assets or information between parties. They are validated using a consensus algorithm, which can vary depending on the specific blockchain implementation. Consensus algorithms are the rules that govern how nodes agree on the contents of the blockchain, including the validation of new transactions and the creation of new blocks. Examples of consensus algorithms include proof-of-work (PoW), proof-of-stake (PoS), and delegated

proof-of-stake (DPoS). Once a transaction is validated, it is added to a block, which is linked to the previous block using cryptographic hashes to form a chain of blocks that cannot be modified without the agreement of the majority of the network. The blockchain database stores the data for each transaction and is linked together using cryptographic hashes to form a chain of blocks. Each block contains a hash of the previous block, creating an unbreakable chain. The database is distributed across all nodes in the network, ensuring that there is no central point of failure or vulnerability. The network protocol is the communication standard that allows nodes to exchange information and maintain the integrity of the blockchain. It ensures that all nodes on the network can communicate with each other securely and efficiently.

The typical flow of transactions between the nodes and the validation and consensus process works as follows (Fig. 3). The user sends a transaction to Node1, which forwards it to the network. The network then

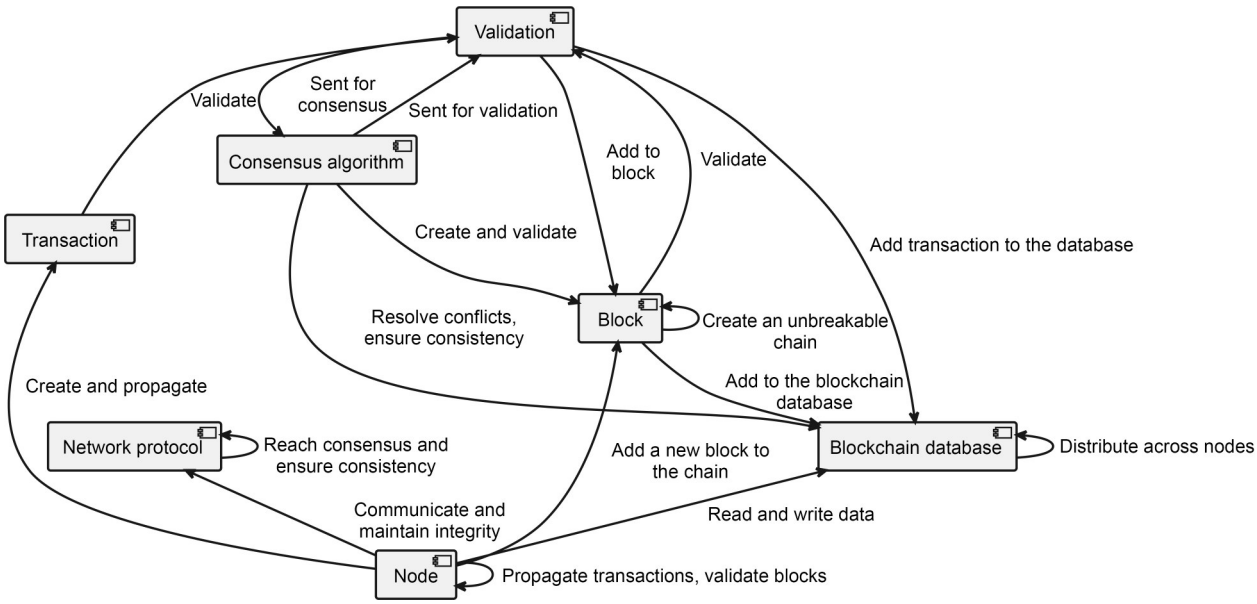

Fig. 2 Components of a blockchain and their relationships

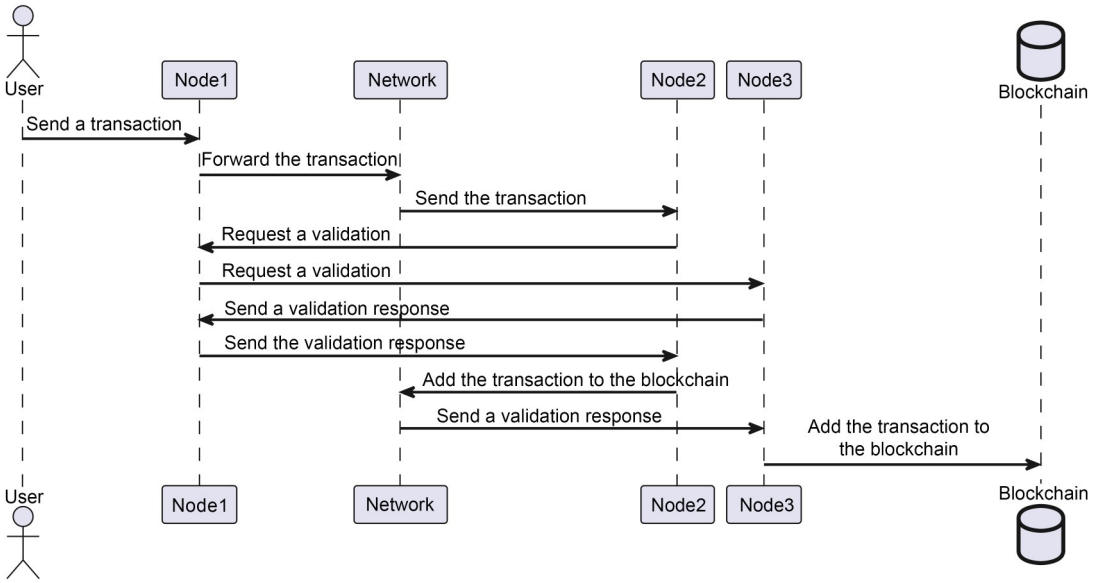

Fig. 3 Typical flow of transactions in a blockchain

sends the transaction to Node2, which requests validation from Node1. Node1 requests a validation from Node3. Node3 sends a validation response to Node1, and then Node1 sends the validation response to Node2. Node2 adds the validated transaction to the blockchain and sends a validation response to the network. The network then sends a validation response to Node3, which adds the validated transaction to the blockchain. The blockchain database stores the data for each transaction and is linked together using cryptographic hashes. Each transaction contains a hash of the previous block, creating an unbreakable chain.

The transaction validation process is shown in Fig. 4. It depicts the flow of transactions and validation within a blockchain network. The actor involved is the user, who initiates the transaction and the various blockchain components, including node, validation, consensus algorithm, blockchain database, and network protocol. The process begins with the user sending a transaction to a node, which then propagates it throughout the network. The node requests a validation from a validation component, which responds with a validation result. The node requests consensus from a consensus algorithm, which sends a consensus result back to the node. Once validated and confirmed by the consensus algorithm, the node adds the transaction to a block, which contains validated transactions. The block is written to the blockchain database, along with the validated transaction. All nodes in the network can read and write to the blockchain database. Throughout the process, the validation component informs the consensus algorithm of the validation result, and the consensus algorithm informs the validation component of the consensus result. The block requests a validation from the validation component. Finally, the network protocol is responsible for sending and receiving data between nodes and maintaining network consensus.

One of the main features of blockchain technology is its ability to create a decentralized and trustless system that removes the need for intermediaries or third parties. In a traditional system, a centralized intermediary, such as a bank, is required to facilitate transactions and ensure the security. However, in a blockchain-based system, transactions are verified and processed by the network of nodes, without the need for a centralized authority. Another key feature of blockchain technology is its immutability, which

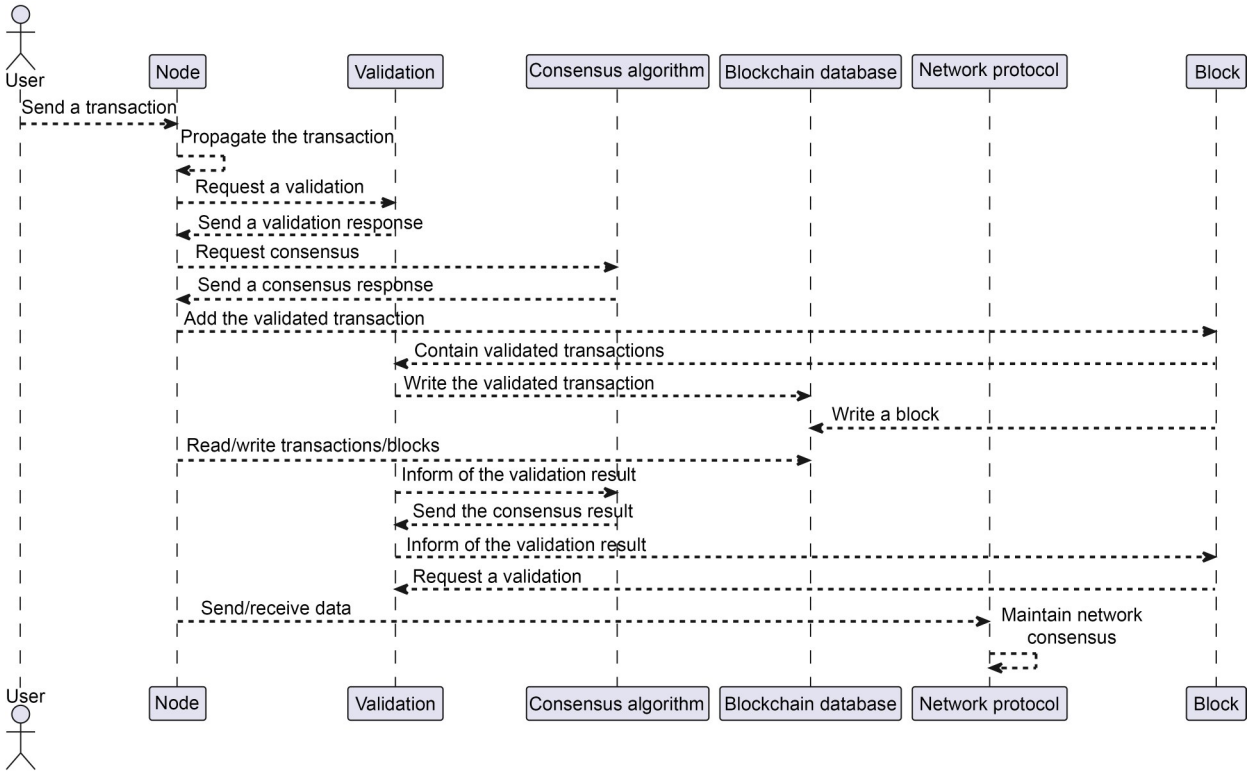

Fig. 4 Validation in a blockchain

means that once a transaction is recorded on the blockchain, it cannot be altered or deleted. This causes blockchain to be a highly secure and tamper-proof system, making it suitable for a wide range of applications, from financial transactions to supply chain management and digital identity verification. Overall, the emergence of blockchain technology has created a new paradigm for secure and transparent data storage and sharing, with numerous potential applications in various industries (Kumar M et al., 2022b).

2.3 Integration of IoT and blockchain

The integration of IoT and blockchain has become popular as businesses and industries seek to enhance the security, scalability, and transparency of their digital infrastructures (Abdelmaboud et al., 2022; Alzoubi et al., 2022; Tanwar et al., 2022). At a basic level, IoT devices generate a massive amount of data, which can be collected, analyzed, and stored in the cloud or on-premises (Murthy et al., 2020). However, traditional centralized data storage and processing methods have significant limitations, including security vulnerabilities and potential data breaches. Blockchain technology provides an innovative solution to these issues by enabling distributed and decentralized storage and processing of data. By integrating IoT and blockchain, businesses can create a more secure and transparent digital infrastructure that allows for real-time data sharing, tracking, and verification (Tran et al., 2021). The decentralized nature of blockchain technology ensures that all parties involved in a transaction have access to the same information, creating a more transparent and trustworthy ecosystem. Blockchain's immutable ledger system ensures that data cannot be tampered with or manipulated, which provides greater security and reliability. One of the key benefits of the integration of IoT and blockchain is the ability to automate transactions through smart contracts (Pradhan et al., 2022b). Smart contracts are self-executing digital contracts that allow for automatic verification and execution of terms and conditions. By incorporating smart contracts into IoT devices, businesses can automate processes, reduce the number of transactions, and increase efficiency (Zubaydi et al., 2023). Another important aspect of IoT and blockchain integration is the ability to track and verify the provenance of goods and products through supply chains. Blockchain provides a tamper-proof record of every transaction (Darbandi et al., 2022), which can be used to track products as they move through the supply chain. This can be particularly useful in industries such as food and beverage or pharmaceuticals, where transparency and traceability are critical for ensuring product safety and quality.

Integration of IoT and blockchain offers a range of benefits for businesses and industries looking to create a more secure, transparent, and efficient digital infrastructure. By leveraging the strengths of both technologies, businesses can create a more trustworthy ecosystem that enables automated transactions, real-time data sharing, and secure product tracking.

3 Layers, threats, and countermeasures of B-IoT

3.1 B-IoT layers and components

The architecture of B-IoT is multi-layered; each layer performs a specific function (Leng et al., 2022). The layers of the B-IoT architecture are as follows:

1. The perception layer includes all the physical objects, sensors, and devices, such as temperature sensors, humidity sensors, motion sensors, and smart cameras, which are parts of the IoT network. The perception layer collects data from the physical world and sends them to the next layer for processing.

2. The network layer includes gateways and routers that manage the flow of data between the perception layer and the other layers of the system. This layer provides network connectivity and protocols for data exchange.

3. The data processing layer includes data storage, processing, and analysis components. It uses various techniques to filter, aggregate, and analyze the data collected from the perception layer and prepare them for use in the application layer.

4. The application layer is the topmost layer of the B-IoT architecture. This layer includes applications that use the data collected from the other layers for specific purposes. These applications could be related to smart homes, smart cities, healthcare, and other domains.

The multi-layered architecture of B-IoT (Fig. 5) provides a systematic approach for designing and

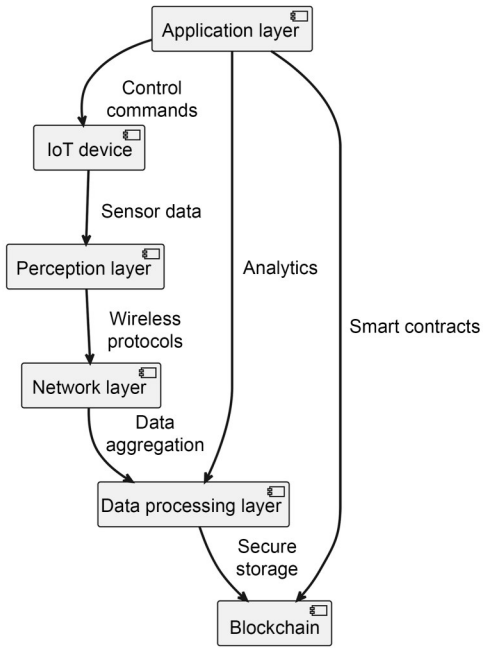

Fig. 5 Generic multi-layered architecture of blockchain-based Internet of Things (B-IoT)

implementing IoT systems that are secure, scalable, and efficient. Each layer of the architecture plays a specific role in the overall system, and the components of each layer work together to achieve the desired functionality.

In this diagram, the B-IoT system is represented as a multi-layered architecture. The IoT device is at the core, interfacing with multiple layers. The perception layer processes sensor data, which are then passed through the network layer using wireless protocols. Data aggregation happens in the network layer and is sent to the data processing layer, where data are securely stored and integrated with the blockchain technology. The application layer, positioned at the top, communicates with both the IoT device and the blockchain through control commands and analytics.

3.2 Threats and attacks on B-IoT

The integration of blockchain and IoT can improve the overall security of IoT systems. However, B-IoT systems are still vulnerable to several threats and attacks that need to be addressed for successful implementation.

One of the primary threats to B-IoT systems is the lack of proper authentication and access control mechanisms (Alzoubi et al., 2022). As B-IoT systems are decentralized, there is a need for secure and robust authentication mechanisms to ensure that only authorized devices can participate in the network. A compromised device can introduce malicious code into the network, leading to security breaches and data theft (Singh et al., 2023). Another significant threat is the lack of data privacy in B-IoT systems (Zubaydi et al., 2023). Data generated by IoT devices are often sensitive, and privacy is critical for user acceptance and adoption. B-IoT systems require strong cryptographic protocols to ensure the privacy and confidentiality of data (Kumar M et al., 2022a, 2022b). Without proper encryption, attackers can easily intercept and access sensitive data, leading to data breaches and financial losses (Hussain et al., 2022).

B-IoT systems are also vulnerable to distributed denial-of-service (DDoS) attacks (Shah et al., 2022). As IoT devices have limited computing power and storage, they are more susceptible to DDoS attacks that can lead to service disruptions and system failures. Attackers can launch DDoS attacks by flooding the network with traffic, leading to an overload of devices and resulting in service disruptions. Malware and ransomware attacks are also significant threats to B-IoT systems (Kshetri, 2017). Malware can infect IoT devices and spread through the network, causing damage and leading to financial losses. Ransomware attacks can encrypt data and demand ransom payments, leading to data and financial losses.

In summary, B-IoT systems are susceptible to various threats and attacks, including lack of authentication and access control, data privacy breaches, DDoS attacks, malware attacks, and ransomware attacks. It is crucial to address these threats to ensure the successful implementation of B-IoT systems.

3.3 Countermeasures to secure B-IoT systems

As discussed in Section 3.2, B-IoT systems face various security threats and attacks, which can cause severe damages to the system and users. Therefore, to ensure the security and privacy of B-IoT systems, several countermeasures have been proposed in the literature. In this subsection, we will discuss some of the essential countermeasures that can be applied to secure B-IoT systems.

3.3.1 Access control

Access control is a fundamental security mechanism that restricts unauthorized access to B-IoT systems (Shi and Li, 2019; Butun and Österberg, 2021;

Bagga et al., 2022). Access control involves identifying and authenticating users, devices, and applications before granting them access to the system resources. Access control can be implemented using various techniques, such as passwords, biometrics, and digital certificates. It also involves the use of role-based access control (RBAC), which restricts users to performing the tasks that are only relevant to their roles in the system.

3.3.2 Encryption

Encryption is another essential countermeasure for securing B-IoT systems (Tanwar et al., 2022). This involves the conversion of plaintext data into a ciphered format to prevent unauthorized access to the data. Encryption can be applied to various components of B-IoT systems, such as data at rest, data in transit, and data in use. The two primary encryption techniques used in B-IoT systems are symmetric key encryption and asymmetric key encryption. Symmetric key encryption involves the use of a single key for both encryption and decryption, whereas asymmetric key encryption uses two keys, i.e., a public key for encryption and a private key for decryption.

3.3.3 Integrity

Integrity is another crucial countermeasure for securing B-IoT systems (Zaman et al., 2022; Singh et al., 2023). This ensures that the data and system resources are not tampered with or modified by unauthorized users. Integrity can be ensured using various techniques, such as hashing and digital signatures. Hashing involves the generation of a unique fixed-length value, known as a hash, for particular input data. Any modification of the input data will result in a different hash value, which indicates data tampering. Digital signatures involve the use of asymmetric key encryption to provide authentication and integrity for digital messages.

3.3.4 Secure communication

Secure communication is essential to protect B-IoT systems from eavesdropping and man-in-the-middle (MitM) attacks. This involves the use of secure communication protocols, such as transport layer security (TLS) and secure sockets layer (SSL), to encrypt the communication between the B-IoT components (Bagga et al., 2022). Secure communication protocols provide end-to-end encryption, ensuring that the communication remains confidential and protected from unauthorized access during data streaming (Venčkauskas et al., 2018).

3.3.5 Security analytics

Security analytics involves the use of data analysis techniques to identify potential security threats and attacks in B-IoT systems (Saba et al., 2022). It uses machine learning (ML) algorithms and artificial intelligence (AI) techniques to analyze the system logs and network traffic to detect anomalies and suspicious activities (Darbandi et al., 2022; Ogundokun et al., 2022b; Alam T, 2023). Security analytics can also be used to predict potential security threats and proactively take measures to prevent them (Li M et al., 2021).

3.3.6 Blockchain technology

Blockchain technology provides an additional layer of security for B-IoT systems by ensuring immutability, transparency, and decentralization. It can be used to store the B-IoT system data, transactions, and logs in a distributed ledger, ensuring that the data cannot be tampered with or modified by unauthorized users. Blockchain technology also provides smart contract functionality, which enables the execution of automated contract terms between different B-IoT components. B-IoT systems face various security threats and attacks, which can cause significant damage to the system and users. Therefore, it is essential to apply appropriate countermeasures to ensure the security and privacy of B-IoT systems. The countermeasures discussed here, such as access control, encryption, integrity, secure communication, security analytics, and blockchain technology, can be used in combination.

3.4 Mathematical models for B-IoT security

In the context of B-IoT, mathematical models can be used to represent security threats and vulnerabilities and to develop efficient security solutions. A mathematical model is essentially a set of equations or algorithms that can be used to simulate the behavior of the system. In the context of B-IoT security, mathematical models can be used to simulate the behavior of various attack scenarios and to evaluate the

effectiveness of different security mechanisms. One of the key challenges in B-IoT security is to develop efficient security mechanisms that can protect against a wide range of attacks. Mathematical models can be used to analyze the security of B-IoT systems and to identify vulnerabilities that could be exploited by attackers. For example, mathematical models can be used to analyze the performance of various encryption and authentication algorithms and to determine the level of security they provide. In addition to analyzing the security of B-IoT systems, mathematical models can be used to develop new security mechanisms. For example, researchers have developed mathematical models that can be used to simulate the behavior of a blockchain-based security system and to evaluate its effectiveness. Mathematical models can also be used to develop new cryptographic algorithms that can provide stronger security guarantees for B-IoT systems. By using mathematical models to analyze and develop security mechanisms, researchers can gain a deeper understanding of the security threats faced by B-IoT systems and develop more effective solutions for protecting these systems from attack.

The Markov chain is a mathematical model that can be used to analyze the behavior of a system over time. It consists of a set of states and transition probabilities between these states. In the context of B-IoT security, the Markov chain can be used to model the behavior of the system with respect to security threats and attacks (Wang X et al., 2019a). The Markov chain model for B-IoT security can be constructed by defining the states of the system based on its security status. For example, a system can be in a secure state, compromised state, or in the process of being compromised. The transition probabilities between these states can be estimated based on the likelihood of a security threat or attack occurring. The Markov chain model can be used to analyze the effectiveness of security measures in the B-IoT system. For example, the model can be used to evaluate the impact of implementing a new security protocol on the overall security of the system. The model can also be used to identify the weakest links in the system and the areas that require the most attention in terms of security.

Suppose that we have a B-IoT system consisting of three layers: the perception layer, network layer, and application layer. Each layer has two states: secure and insecure. We can represent the states of the B-IoT system using a Markov chain as follows: Assuming that we have N states in the Markov chain model, the state transition probabilities can be represented by the transition probability matrix $\boldsymbol{P}$:

$$\boldsymbol{P}=[p_{ij}],\ i,j=1,2,...,N,$$

where p_{ij} is the probability of transitioning from state i to state j. Let $\boldsymbol{X}(t)=[x_1(t), x_2(t), ..., x_N(t)]$ be the state vector at time t. Then, the Markov chain model can be described by the following equation:

$$\boldsymbol{X}(t+1)=\boldsymbol{X}(t)\boldsymbol{P}.$$

To incorporate security into the model, we can assign a security level to each state, representing the level of security associated with the corresponding state. Let $\boldsymbol{S}=[s_1, s_2, ..., s_N]$ be a vector representing the security levels of the N states. Then, the overall security level of the system at time t can be computed as

$$\text{Security}(t)=\boldsymbol{X}(t)\boldsymbol{S}^{\mathrm{T}}.$$

To analyze the security of the system, we can use various techniques such as analyzing the steady-state probabilities, computing the expected time to reach a certain security level, or analyzing the effect of perturbations on system security. In this Markov chain, each state represents a particular configuration of the B-IoT system. For example, state 1 represents a B-IoT system where the perception layer and network layer are both secure and the application layer may be in either a secure or insecure state. The transitions between states represent the probability of moving from one configuration to another. For example, if the B-IoT system is in state 1, there is a certain probability of transitioning to state 2, where the perception layer is secure but the network layer is insecure. Using the Markov chain model, we can compute the probability of the B-IoT system being in a particular state at a given time. We can also use the model to analyze the behavior of the B-IoT system under different conditions, such as changes in the security of individual layers or the overall system. This analysis can help us identify potential vulnerabilities in the B-IoT system and design more effective security solutions.

4 Blockchain-based security solutions in IoT

4.1 Smart contracts and decentralized control

Smart contracts and decentralized control are two blockchain-based security solutions that can be used in IoT to enhance security and privacy.

Smart contracts are self-executing contracts that are built on top of blockchain technology (Singh et al., 2023). They are automated programs that run on a blockchain network and are designed to facilitate, verify, and enforce the negotiation or performance of a contract. Smart contracts can be used in IoT to automate the execution of certain tasks and enforce specific conditions or rules. For example, a smart contract could be programmed to automatically release payment once a certain condition is met, such as the successful delivery of a product. This can help reduce the risk of fraud and errors, and improve efficiency and transparency (Xiong et al., 2022).

Decentralized control is another blockchain-based security solution that can be used in IoT (Singh et al., 2023; Zhang et al., 2023). Decentralized control refers to the distribution of control and decision-making power across a network, rather than relying on a single central authority or entity. In the context of IoT, decentralized control can be achieved through the use of blockchain technology, which allows for the creation of a decentralized network of devices that can communicate and share data securely and transparently. This can help prevent unauthorized access or tampering, and improve resilience and scalability.

4.2 Immutable data storage

Immutable data storage is a key aspect of blockchain-based security solutions in IoT. In traditional data storage systems, data can be easily altered or deleted, creating security vulnerabilities. However, with blockchain, data are stored in a tamper-proof and immutable way. Once data are added to the blockchain, they cannot be modified or deleted without the consensus of the network, making them highly secure. In the context of IoT, immutable data storage can be used to store important information such as sensor data, device logs, and transaction records. For example, in a supply chain management system, blockchain can be used to store information about the origin and history of a product. This information can be securely accessed by stakeholders throughout the supply chain, providing transparency and traceability. One of the benefits of immutable data storage in blockchain is that it provides a high level of integrity and authenticity. Data stored on the blockchain can be verified as authentic, and the source of the data can be traced back to its origin. This makes it difficult for malicious actors to tamper with or forge data.

4.3 Identity and access management

IAM is a security solution that helps manage user access to systems, networks, and applications. IAM can be implemented in B-IoT systems using blockchain technology to ensure that identities are secure and tamper-proof. IAM provides secure access control to B-IoT devices and networks, ensures privacy, and protects against unauthorized access. In a blockchain-based IAM system, each user has a unique identity that is stored on the blockchain. The user's identity is verified through the use of digital signatures and private keys, which are securely stored on the blockchain. The user's identity and access rights are then associated with a smart contract that is stored on the blockchain. In addition to access control, IAM can be used to manage device identities. Each device in the B-IoT system can be assigned a unique identity that is stored on the blockchain. This identity can be used to authenticate the device and ensure that it is communicating with authorized nodes in the network.

By using blockchain technology for IAM, B-IoT systems can benefit from enhanced security, transparency, and privacy. The use of digital signatures and smart contracts ensures that access control policies are enforced consistently and transparently, while the use of immutable data storage ensures that identities are secure and tamper-proof.

4.4 Consensus mechanisms

Consensus mechanisms play a vital role in ensuring the security and integrity of the data stored in a B-IoT system (Ferrag and Shu, 2021). In a decentralized network, where there is no centralized authority, a consensus mechanism is required to validate transactions and maintain the integrity of the data (Wadhwa et al., 2022). Consensus mechanisms ensure that all nodes in the network have a copy of the same data and that no malicious actors can alter the data without being

detected. There are different types of consensus mechanisms used in B-IoT systems, including PoW, PoS, DPoS, and practical Byzantine fault tolerance (PBFT). PoW is the most well-known and widely used consensus mechanism in blockchain-based systems, including Bitcoin and Ethereum. In PoW, nodes in the network compete to solve complex mathematical problems, and the first node to solve the problem gets to add the next block to the blockchain. This process is energy-intensive and slow, which is why other consensus mechanisms, such as PoS and DPoS, have emerged. PoS and DPoS use a different approach to achieving consensus in the network. In PoS, nodes are selected to validate transactions based on the amount of cryptocurrency they hold, while in DPoS, nodes are elected by the community to validate transactions. Both PoS and DPoS are faster and more energy-efficient than PoW, but they require a high level of trust in the nodes selected to validate transactions. PBFT is a consensus mechanism used in permissioned blockchain networks, where nodes are known and trusted. In PBFT, nodes in the network agree on the order of transactions through a voting process, and the transactions are added to the blockchain once a majority of nodes agree on the order. Overall, consensus mechanisms are a critical component of B-IoT systems and ensure that the data stored in the network are secure and immutable (Bagga et al., 2022).

5 Use cases and applications of B-IoT

B-IoT has multiple applications (Krichen et al., 2022). In this article, we discuss only a few of them.

5.1 Supply chain management

B-IoT has immense potential to transform the supply chain industry by increasing transparency, traceability, and efficiency (Arias-Aranda et al., 2021; Leng et al., 2022). The decentralized nature of blockchain and the real-time tracking and monitoring capabilities of IoT can help streamline the supply chain processes and reduce costs. One application of B-IoT in supply chain management is the tracking and tracing of goods from the point of origin to the final destination. By leveraging radio frequency identification (RFID) sensors and blockchain technology, supply chain managers can track and monitor the movement of goods, ensuring that they are delivered in a timely and secure manner. This can help reduce the risk of theft, loss, and counterfeiting while improving the overall efficiency of the supply chain. Another application of B-IoT in supply chain management is the optimization of inventory management. By using IoT sensors to monitor inventory levels in real time and blockchain technology to securely store and share data, supply chain managers can optimize inventory levels, reduce the risk of stockouts, and increase efficiency. Smart contracts can also be used in supply chain management to automate various processes, such as payment and delivery. By using blockchain-based smart contracts, supply chain managers can ensure that payments are made only when goods are delivered, reducing the risk of fraud and improving transparency.

Further, we discuss an example scenario of an inventory management system implemented on B-IoT (Fig. 6).

In this scenario, a user requests an update on inventory levels from the inventory system. The inventory system retrieves inventory data from the blockchain, which provides a secure and tamper-proof record of inventory levels. The inventory system then displays the inventory data to the user. When the user requests a purchase order, the inventory system sends a transaction to the blockchain to confirm the purchase order. The blockchain confirms the transaction and sends the confirmation back to the inventory system, which then sends a confirmation of the purchase order to the user.

This process ensures that inventory levels are accurately tracked and that purchase orders are securely and transparently processed.

B-IoT has the potential to transform the supply chain industry by increasing transparency, traceability, and efficiency, while reducing costs and improving customer satisfaction.

5.2 Healthcare and assisted living

The integration of blockchain technology and IoT has several applications in healthcare and assisted living, offering solutions for data security, privacy, and trust (Bigini et al., 2020; Ratta et al., 2021; Alam S et al., 2022). For example, blockchain was adopted

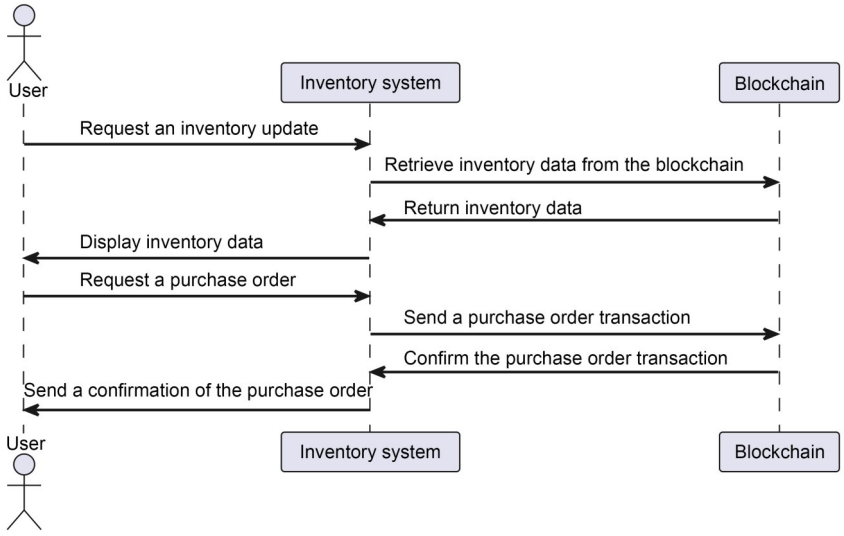

Fig. 6 An example of an inventory management system implemented using blockchain-based Internet of Things (B-IoT)

for COVID-19-related information sharing (Aslan and Ataşen, 2021) and ensuring authenticity of vaccine vials (Chauhan et al., 2021). Here are some of the applications of B-IoT in healthcare and assisted living:

1. Medical data management. The use of B-IoT can improve the management of medical data, including electronic health records, medical images (Praveen et al., 2022; Vulli et al., 2022), and other health-related information (Srinivasu et al., 2021). With blockchain technology, medical data can be securely stored and shared among healthcare providers, patients, and other authorized parties (Pradhan et al., 2022a).

2. Clinical trials. Blockchain technology can be used to improve the efficiency and transparency of clinical trials. The use of smart contracts can help automate the process of data collection, patient recruitment, and compensation for participants (Ghosh et al., 2023). The immutable nature of the blockchain ensures that all data are tamper-proof and transparent, improving the credibility of the results.

3. Medication tracking and authentication. B-IoT can be used to track the medication supply chain, ensuring that drugs are authentic and not counterfeit (Kumar M et al., 2022b). By placing sensors on medication packaging, the blockchain can record the movement of drugs from the manufacturer to the patient, ensuring that the medication has not been tampered with.

4. Remote patient monitoring. IoT devices can be used to monitor patients remotely, collecting data on vital signs, medication compliance, and other health-related metrics (Ghosh et al., 2023). The use of blockchain technology ensures that these data are secure and private, providing patients with more control over their health data.

5. Assisted living. B-IoT can be used to create smart homes that cater to the needs of elderly and disabled individuals. Sensors can be placed throughout the home to monitor the individual's movements and detect falls (Florea et al., 2022). The data collected by these sensors can be securely stored on the blockchain, ensuring the privacy and security of the individual's health data.

Further, we describe an example scenario of a remote patient monitoring system implemented on B-IoT (Fig. 7).

In this scenario, the patient wears a device that collects data on his/her health, such as heart rate and activity levels. These data are sent to a gateway, which then stores them on the blockchain for secure and tamper-proof storage. Healthcare providers can then access these data by querying the blockchain. The gateway sends a query to the wearable device to display the data to the patient. This allows for remote patient monitoring, allowing healthcare providers to monitor the patient's health status and adjust treatment plans as necessary.

Overall, the integration of B-IoT in healthcare and assisted living can improve the efficiency, transparency, security of medical data management, and the quality of life for patients.

5.3 Energy and utilities

B-IoT can be used in energy and utility management to increase efficiency, transparency, and security (Pradhan et al., 2022a, 2022b; Li J et al., 2023). Here are some potential applications of B-IoT in this field:

1. Smart grid management. B-IoT can be used to build smart grids that allow for more efficient and reliable energy distribution. Devices such as smart meters and sensors can be integrated into the grid to monitor energy consumption and identify areas of wastage. The data collected can be stored on the blockchain, providing a tamper-proof record that can be used for auditing and verification purposes.

2. Renewable energy trading. With B-IoT, renewable energy sources such as solar panels and wind turbines can be connected to the grid and their output can be tracked and recorded on the blockchain. This allows for the creation of a decentralized energy marketplace where excess energy can be sold to other consumers.

3. Asset tracking. B-IoT can be used to track energy assets such as power plants, transformers, and transmission lines. The data collected can be used to identify maintenance needs and predict failures, reducing downtime and increasing overall system efficiency.

4. Billing and payment. With B-IoT, energy consumption can be accurately measured and recorded on the blockchain, enabling automatic billing and payment processing. This eliminates the need for manual meter readings and reduces the risk of fraud.

5. Demand response. B-IoT can be used to monitor and manage energy demand in real time. By using smart devices such as thermostats and lighting controls, energy consumption can be reduced during periods of peak demand, reducing strain on the grid and avoiding blackouts.

Further, we describe an example scenario of how B-IoT could be used in a smart grid management system (Fig. 8). The smart grid system consists of smart meters, sensors, and other IoT devices that are connected to the grid. The data collected by these devices are stored on the blockchain, providing a secure and tamper-proof record of energy consumption and distribution. The system can analyze these data to identify areas of high energy consumption and

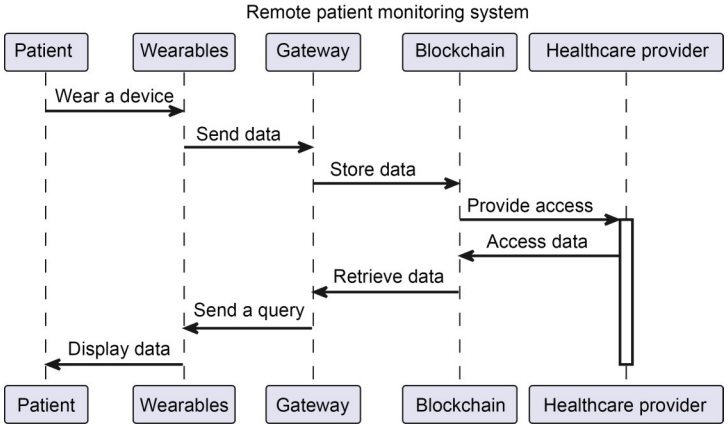

Fig. 7 An example of a remote patient monitoring system implemented on blockchain-based Internet of Things (B-IoT)

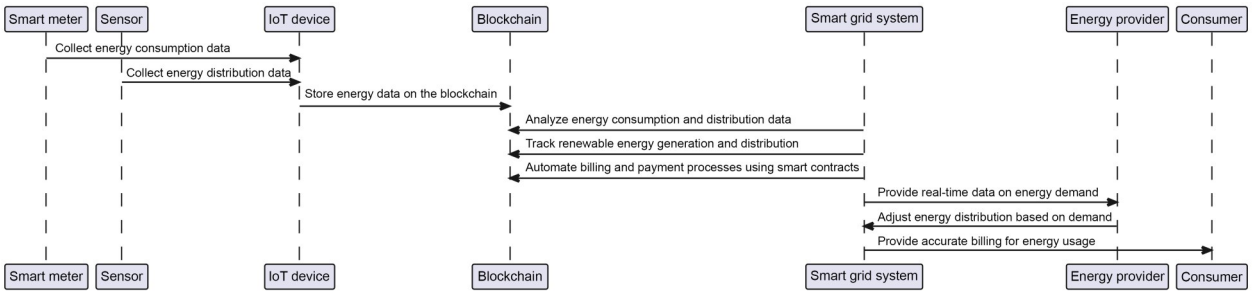

Fig. 8 An example of smart grid management using blockchain-based Internet of Things (B-IoT)

wastage, allowing for more efficient distribution and usage of energy. The blockchain can also be used to track the generation and distribution of renewable energy sources such as solar and wind power. Smart contracts can be used to automate billing and payment processes, ensuring that consumers are accurately charged for their energy usage. The system can also provide real-time data on energy demand and adjust energy distribution accordingly, reducing the risk of blackouts and other disruptions. With B-IoT, the smart grid system is more efficient, transparent, and secure, providing benefits to both energy providers and consumers.

5.4 Smart cities and transportation

B-IoT has the potential to revolutionize the way we live and work and interact with the world around us. Smart cities and transportation are two areas where B-IoT can make a significant impact (Sunny et al., 2022; Alam T, 2023). In a smart city, B-IoT can be used to monitor and manage various aspects of the urban environment, such as traffic flow, energy consumption, waste management, and air quality. By collecting and analyzing data from various sensors and devices, B-IoT can help city administrators make more informed decisions about how to allocate resources and respond to emergencies. For example, in a traffic management system, B-IoT can be used to collect real-time data about traffic flow, road conditions, and accidents. These data can be analyzed to optimize traffic flow, reduce congestion, and improve safety. In a waste management system, B-IoT can be used to monitor trash levels in bins and optimize garbage collection routes, reducing costs and environmental impact.

In transportation, B-IoT can be used to improve safety, efficiency, and sustainability. By collecting and analyzing data from sensors and devices on vehicles, B-IoT can provide insights into driver behavior, road conditions, and vehicle performance. For example, in a fleet management system, B-IoT can be used to monitor the location, speed, and fuel consumption of vehicles. These data can be analyzed to optimize routes, reduce fuel consumption, and improve safety. In a transportation network, B-IoT can be used to monitor traffic flow and provide real-time updates to drivers, reducing congestion and travel time. Thus, B-IoT has the potential to transform smart cities and transportation by providing a wealth of data and insights that can be used to optimize resources, improve safety, and reduce environmental impact. However, it is important to address the challenges and vulnerabilities associated with B-IoT to ensure its successful implementation in these areas.

We present and analyze an example scenario of a traffic management system implemented on B-IoT (Fig. 9).

The traffic management system collects real-time traffic data from various IoT devices such as traffic sensors, global positioning system (GPS) trackers, and cameras. The data collected are transmitted to the network layer of the B-IoT system, where they are processed and analyzed to identify traffic patterns, congestion, and other traffic-related issues. The analyzed data are then transmitted to the data processing layer, where they are further processed and aggregated

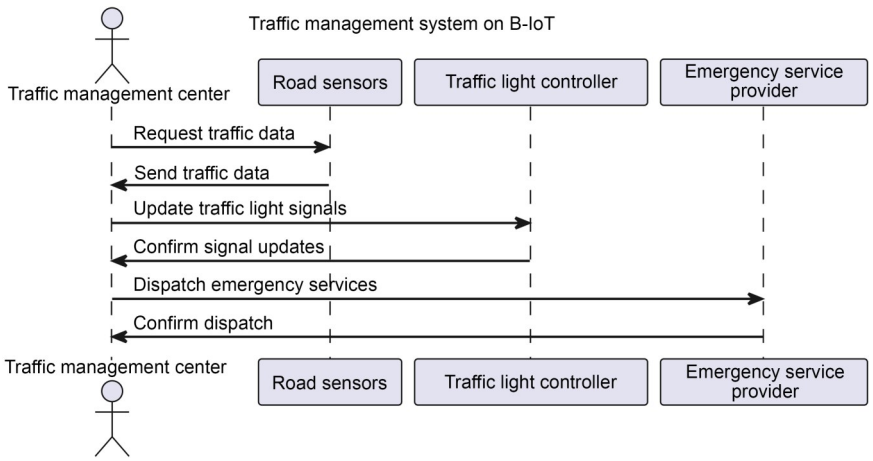

Fig. 9 An example of a traffic management scenario using blockchain-based Internet of Things (B-IoT)

to generate insights and predictions about future traffic conditions. Based on the generated insights, the application layer of the B-IoT system takes actions to optimize traffic flow and reduce congestion, such as adjusting traffic signals, redirecting traffic, and providing real-time traffic updates to drivers. The B-IoT system also leverages blockchain technology to ensure the security and integrity of the collected data and the actions taken based on them.

In this scenario, the traffic management center is the actor that initiates the traffic management process. The traffic management center requests traffic data from the road sensors, which send the data back to the traffic management center. The traffic management center then updates the traffic light signals through the traffic light controller and confirms the updates with the controller. If there is an emergency situation, the traffic management center dispatches emergency services and confirms the dispatch with the emergency service provider. This sequence diagram represents the interactions between the different components in a traffic management system implemented on B-IoT. Therefore, the B-IoT-based traffic management system provides a comprehensive and efficient solution for managing traffic in real time, improving traffic flow, and reducing congestion on the roads.

6 Challenges and limitations in B-IoT

6.1 Scalability issues

Scalability is a significant challenge that arises when integrating blockchain with the IoT (Kashyap et al., 2022; Taherdoost, 2023). The B-IoT network must be able to manage a large number of devices that generate a tremendous amount of data. A blockchain can become congested and slow when it is overwhelmed by a large number of transactions, which can impact the performance and efficiency of the IoT devices connected to it. One of the primary reasons for scalability issues in B-IoT is the consensus mechanism. Traditional consensus algorithms like PoW and PoS are not suitable for B-IoT networks because they are computationally intensive and require a lot of energy to operate. As a result, they can lead to long processing time and high transaction costs, which are detrimental to IoT applications. To address scalability issues, new consensus algorithms, such as proof of elapsed time (PoET), DPoS, and PBFT, have been developed. These algorithms are designed to be more energy-efficient and faster than traditional consensus algorithms, which can help improve the scalability of B-IoT networks. Another approach to improving scalability in B-IoT is through the use of off-chain scaling solutions. These solutions involve moving some of the transaction processing off the main blockchain network, which can help reduce congestion and improve the overall performance of the network. In summary, scalability is a significant challenge in B-IoT due to the large number of IoT devices connected to the network and the amount of data generated by these devices. To address this challenge, new consensus algorithms and off-chain scaling solutions are being developed to improve the scalability of B-IoT networks.

6.2 Security vulnerabilities

Despite its potential advantages, B-IoT is vulnerable to various security threats due to its distributed and decentralized nature (Altaf et al., 2023; Singh et al., 2023). These vulnerabilities include the following:

1. Sybil attacks occur when a malicious actor creates multiple fake identities to take control of a network or generates false data to manipulate the system.

2. Denial-of-service (DoS) attacks involve overwhelming the network with a flood of requests, making it unavailable to legitimate users (Ali et al., 2022; Shah et al., 2022).

3. Eavesdropping and MitM attacks: Eavesdropping occurs when an attacker intercepts the communication between two devices, while an MitM attack occurs when an attacker intercepts and alters the communication between two devices.

4. Tampering involves unauthorized changes to data or device configurations, leading to the loss of integrity and confidentiality of data.

5. Insider attacks are carried out by an authorized user who exploits his/her access to the network to cause harm.

6. Botnet attacks are any attack that distributes resources and scales operations using a botnet—a network of bots and devices connected together to achieve the same objective (Alharbi et al., 2021).

These security vulnerabilities could have severe consequences, such as data theft, unauthorized access,

and other types of malicious activities, which could compromise the integrity and confidentiality of data and the availability and performance of the system. It is, therefore, essential to implement appropriate security measures to address these vulnerabilities and ensure the safety and integrity of the B-IoT system and security awareness (Grigaliunas et al., 2021). Such measures may include the use of encryption, access control, and blockchain-based solutions such as smart contracts, consensus mechanisms, and identity management.

6.3 Convergence challenges

Convergence is a critical aspect of the B-IoT ecosystem, which refers to the integration of various technologies and devices in a unified network to achieve a common goal (Maroufi et al., 2019). Convergence of B-IoT systems presents significant challenges that need to be addressed to ensure efficient and effective functioning. Some of the critical convergence challenges in B-IoT include the following:

1. Interoperability. It refers to the ability of different B-IoT systems and devices to communicate and share data seamlessly across different platforms. However, different B-IoT devices and platforms are built using different protocols, standards, and technologies, making it difficult for them to communicate and interoperate effectively. Interoperability issues can lead to data loss, system downtime, and security breaches.

2. Scalability. B-IoT networks are expected to grow exponentially in the future, which raises scalability challenges for the system. Scalability refers to the ability of a system to accommodate increasing amounts of data and traffic without compromising its performance or efficiency. However, the decentralized nature of B-IoT systems presents scalability challenges, because the processing power and storage capacity of each node are limited.

3. Security. B-IoT systems are highly vulnerable to security breaches due to their distributed and decentralized nature, which makes them more susceptible to cyberattacks, data theft, and other security threats. Security convergence challenges arise when different B-IoT devices and systems need to communicate and share data securely across the network.

4. Data management. B-IoT systems generate vast amounts of data that need to be collected, processed, and managed effectively to achieve their objectives. However, convergence challenges arise when different B-IoT devices and platforms use different data formats, storage mechanisms, and processing methods.

Addressing convergence challenges in B-IoT requires collaboration among various stakeholders, including device manufacturers, software developers, standards organizations, and regulatory bodies. Some of the proposed solutions for addressing convergence challenges in B-IoT include the use of open standards, common protocols, and interoperability frameworks. Additionally, the integration of AI and ML techniques in B-IoT systems can help improve their performance, scalability, and security (Atlam et al., 2020; Ogundokun et al., 2022a).

6.4 Computational complexity and energy efficiency

The integration of blockchain and IoT introduces various challenges, such as the need for efficient resource utilization, including memory space and processing power. Different blockchain methods may have varying computational requirements, which can impact the performance of IoT systems. Some techniques, such as PoW, are known to be computationally intensive, requiring significant amounts of computational power and time for mining and validating blocks. This can result in higher energy consumption and longer transaction processing time. Alternative consensus mechanisms like PoS or DPoS aim to address the computational complexity and energy inefficiency issues associated with PoW. These methods typically require less computational power and energy consumption, making them more suitable for resource-constrained IoT devices.

6.4.1 Computational complexity of blockchain consensus mechanisms

The computational complexity of blockchain consensus mechanisms can be analyzed using Big-O notation, which provides a way to express the scalability and efficiency of algorithms as the size of the input grows. Different consensus mechanisms have varying computational complexities, impacting the performance and resource requirements of the blockchain system (Bamakan et al., 2020).

PoW is one of the most widely known consensus mechanisms, and is used in cryptocurrencies like

Bitcoin. The computational complexity of PoW is typically expressed as $O(n)$, where n represents the number of computations required to find a valid hash that satisfies the difficulty criteria. The difficulty level is adjusted to maintain a consistent block creation time, which affects the computational effort and energy consumption required for mining.

PoS is an alternative consensus mechanism that selects validators based on their stake or ownership of cryptocurrency. The computational complexity of PoS is generally expressed as $O(1)$ since the selection process does not depend on solving complex mathematical puzzles. However, the precise complexity may vary depending on the specific implementation.

DPoS is a variation of PoS where a limited number of trusted validators are elected to validate transactions and produce blocks. The computational complexity of DPoS is also expressed as $O(1)$, because the validator selection process is typically based on voting or reputation.

PBFT is a consensus mechanism used in permissioned blockchain networks. It achieves consensus through a series of rounds of message exchanges and voting. The computational complexity of PBFT is expressed as $O(n^2)$, where n represents the number of participating nodes. The quadratic complexity arises due to the need for message exchanges and multiple rounds of voting.

Proof of weight (PoWeight) is a blockchain consensus mechanism that incorporates elements from other consensus mechanisms, such as PoS. Participants' influence or weight in the network is determined by factors like the number of tokens they hold or their reputation. This mechanism aims to achieve consensus by giving more decision-making power to participants with higher weight, promoting a more decentralized and democratic network. The computational complexity of PoWeight depends on the specific implementation, because it combines elements of other consensus mechanisms. For example, if PoWeight incorporates PoS, the computational complexity would be similar to that of PoS, typically expressed as $O(1)$, because the selection process does not involve solving complex mathematical puzzles.

Proof of burn (PoB) is a consensus mechanism where participants demonstrate their commitment to the network by burning or destroying a certain number of cryptocurrency tokens. This action is irreversible and provides proof of dedication and trustworthiness. PoB encourages long-term commitment to the network and can reduce the influence of participants who may try to manipulate the system by acquiring a large number of tokens. The computational complexity of PoB is generally expressed as $O(1)$, because the burning process does not involve complex computations or cryptographic puzzles. It mainly requires the destruction or sacrifice of cryptocurrency tokens to prove commitment to the network.

Proof of capacity (PoC) is a consensus mechanism that uses participants' available storage capacity to determine their mining power (Dziembowski et al., 2015). Participants allocate a portion of their storage space to the blockchain network, and mining operations are performed based on this allocated capacity. PoC is known for its energy efficiency, because it requires less computational power compared to other mechanisms like PoW, making it more environmentally friendly. The computational complexity of PoC is primarily determined by the storage and retrieval operations associated with the allocated disk space or storage capacity. The complexity is typically expressed as $O(n)$, where n represents the amount of storage space allocated for mining.

Proof of importance (PoI) is a consensus mechanism that takes into account participants' importance or reputation within the network. It considers factors like transaction history, network activity, and stake in the system to determine the weight of participants. By giving more influence to active and committed participants, PoI aims to achieve consensus in a way that aligns with the best interests of the network and its stakeholders. The computational complexity of PoI varies depending on the specific implementation. In PoI, the selection of participants for block validation is influenced by their importance in the network, often considering factors such as transaction history and network activity. The exact complexity would depend on the algorithm used to calculate the importance score.

These complexities represent the computational effort required for the consensus mechanism itself and do not account for additional overheads introduced by network communication, data storage, or transaction processing.

6.4.2 Energy efficiency of blockchain consensus mechanisms

Energy efficiency is a critical consideration in blockchain consensus mechanisms, particularly as energy consumption has become a significant concern in blockchain networks (Sedlmeir et al., 2020). PoW consensus mechanisms, such as those used in Bitcoin, are known for their high energy consumption. The energy efficiency of PoW is typically measured by the ratio of energy expended to secure the network versus the number of transactions processed. The higher the computational complexity of PoW, the more the energy it consumes to solve the cryptographic puzzles and validate blocks.

PoS consensus mechanisms offer potential improvements in energy efficiency compared to PoW. In PoS, energy consumption is significantly reduced as the consensus process relies on participants' stake or ownership of cryptocurrency, rather than extensive computational work. However, the energy efficiency of PoS can vary depending on the specific implementation and the distribution of stakes among participants.

DPoS is another consensus mechanism that aims to enhance energy efficiency. DPoS reduces the number of participants involved in block validation, allowing for shorter block confirmation time and lower energy consumption compared to PoW and PoS. By relying on a limited number of trusted validators, DPoS reduces the computational and energy requirements for consensus.

PBFT, used in permissioned blockchain networks, achieves consensus through a series of message exchanges and voting. Although PBFT offers high throughput and low latency, its energy efficiency depends on the number of participating nodes and the communication overheads incurred during the consensus process.

PoWeight's energy efficiency depends on the underlying consensus mechanisms it incorporates. If it incorporates energy-efficient mechanisms like PoS, it can offer improved energy efficiency compared to energy-intensive mechanisms like PoW. However, the energy efficiency can still vary based on the implementation details and the distribution of weights among participants.

PoB is often considered energy-efficient as it does not require extensive computational work like PoW. By burning existing tokens, participants demonstrate a financial commitment, reducing the need for energy-intensive mining activities. As a result, PoB can offer improved energy efficiency compared to PoW.

PoC is known for its energy efficiency because the mining process relies mainly on the capacity to store and retrieve data. It requires significantly less computational power compared to PoW and PoS, resulting in reduced energy consumption during the mining process.

PoI can offer improved energy efficiency compared to energy-intensive consensus mechanisms like PoW. By considering factors beyond computational power, such as network participation and activity, PoI encourages stakeholder involvement and reduces the need for extensive computational work, thereby improving energy efficiency. In assessing energy efficiency, it is crucial to consider not only the consensus mechanism but also the underlying infrastructure, including hardware specification, network protocols, and system optimization. Furthermore, the energy efficiency of a blockchain network can be influenced by factors such as transaction volume, block size, and the efficiency of participating nodes (Bada et al., 2021).

6.4.3 Computational complexity of cryptographic algorithms in blockchain

Cryptographic algorithms play a crucial role in ensuring the security and integrity of blockchain systems in IoT. Evaluating their computational complexity and energy efficiency is essential for understanding their feasibility and impact on resource-constrained IoT devices.

Hash functions are widely used in blockchain to ensure data integrity and create unique identifiers for transactions and blocks. Commonly used hash functions, such as SHA-256, have a computational complexity of $O(1)$ for generating a hash value. The complexity remains constant regardless of the input size.

Asymmetric key algorithms, like Rivest–Shamir–Adleman (RSA) or elliptic curve cryptography (ECC), are used for digital signatures, key exchange, and encryption. The computational complexity of these algorithms is typically expressed as $O(n^3)$ or $O(n^2)$,

where n represents the size of the key. The complexity arises from mathematical operations like modular exponentiation and point multiplication.

Symmetric key algorithms, such as advanced encryption standard (AES), are used for encrypting data within blockchain systems. The computational complexity of symmetric key encryption and decryption is generally expressed as $O(1)$, because the operations are highly optimized and a constant number of operations are required regardless of the input size.

6.4.4 Energy efficiency of cryptographic algorithms in blockchain

When considering energy efficiency, it is important to note that computational complexity alone does not directly translate into energy consumption. Factors such as the key size, hardware implementation, efficiency of the cryptographic library, and device-specific optimization play significant roles in determining energy efficiency (Vračar et al., 2019). In terms of energy efficiency, symmetric key algorithms tend to be more efficient compared to asymmetric key algorithms. Symmetric key operations require less computation amount and have lower energy requirements. To improve energy efficiency in IoT devices, lightweight cryptographic algorithms have been developed, such as lightweight cryptography (LWC) algorithms. These algorithms are specifically designed to minimize computational complexity and energy consumption, making them suitable for resource-constrained IoT devices (Nyangaresi et al., 2022). By understanding these trade-offs, researchers, practitioners, and system designers can make informed decisions when selecting the most suitable blockchain method for IoT applications, considering the computational constraints and efficiency requirements of their specific use cases.

7 Ethical and social issues of B-IoT

7.1 Privacy and data protection

The integration of IoT and blockchain has brought significant benefits in terms of security and data integrity. However, this integration also raises privacy and data protection concerns that need to be addressed. Some of the key privacy and data protection issues in B-IoT include the following:

1. Pseudonymity. In blockchain-based systems, users are identified by their public keys, which are not linked to their real identities. Although this provides a degree of anonymity, it also makes it difficult to enforce privacy regulations such as general data protection regulation (GDPR), that require individuals to have the right to know what data are being collected about them (Conoscenti et al., 2016).

2. Data leakage. The decentralization of data storage in blockchain-based systems can lead to data leakage. For example, in a permissionless blockchain, any node can access and download the entire blockchain. This can lead to the exposure of sensitive data, such as personal information (Deepika et al., 2022).

3. Data ownership. In B-IoT systems, multiple parties may have access to the same data. This can lead to issues around data ownership and control. It is important to establish clear guidelines around data ownership, access, and control to ensure that data are not misused (Bigini et al., 2020).

4. Interoperability. B-IoT systems often involve multiple devices and platforms, which can lead to interoperability issues. For example, data from one IoT device may need to be combined with data from another device to provide a complete picture. Ensuring that data can be easily shared and combined across different devices and platforms while maintaining privacy is a significant challenge (Abdelmaboud et al., 2022).

5. Data breaches. B-IoT systems are vulnerable to data breaches, which can result in the exposure of sensitive data. It is important to implement robust security measures to prevent unauthorized access to data (Rahmani et al., 2022).

To address these privacy and data protection issues, B-IoT systems need to incorporate privacy-enhancing technologies, such as encryption and data obfuscation. Additionally, clear guidelines concerning data ownership and access need to be established, and security measures need to be implemented to prevent data breaches. Finally, B-IoT systems should be designed with privacy and data protection in mind from the outset, rather than being retrofitted with privacy features after deployment.

7.2 Ownership and control of data

In the context of B-IoT, ownership and control of data refer to the rights and control that various entities have over the data generated by IoT devices, respectively. As IoT devices continue to proliferate, the amount of data they generate will increase exponentially. These data can be valuable to a wide range of stakeholders, including businesses, governments, and individuals. One of the primary concerns with B-IoT is that the ownership and control of data may not be clear. In many cases, the devices generating the data may be owned by individuals or businesses, while the data themselves may be collected and stored by third-party providers. This can create ambiguity concerning who has the right to access and use the data and who is responsible for protecting them. One potential solution to this issue is the use of blockchain technology. By using a decentralized ledger, data can be securely stored and tracked, ensuring that only authorized parties have access to them. Additionally, smart contracts can be used to specify the terms of data access and usage, providing clear rules and transparency around ownership and control. However, there are still significant challenges to overcome in terms of establishing clear ownership and control of data in B-IoT systems. These include technical challenges related to data standardization and legal and regulatory challenges related to data privacy and intellectual property rights. As B-IoT continues to develop and mature, addressing these challenges will be critical to ensuring that data are used in a way that benefits all stakeholders.

7.3 Trust and transparency

Trust and transparency are important issues in any system that involves the sharing of data between different entities. In the context of B-IoT, trust refers to the confidence that each entity has in the other entities in the system, and transparency refers to the ability to verify the actions of each entity and the data that they are sharing. One of the main challenges in B-IoT is establishing trust between different entities in the system (Zhang et al., 2023). This is especially true when the entities are not known to each other, such as when a device from one company connects to a network owned by another company. To establish trust, it is important to have a clear set of rules and procedures for sharing data and mechanisms in place to ensure that these rules are followed (Rahmani et al., 2022). This could include the use of smart contracts or other blockchain-based technologies to enforce rules for the sharing of data and ensure that all parties are acting in good faith. Transparency is also an important issue in B-IoT, because it is important to be able to verify the actions of each entity in the system (Zaman et al., 2022). This includes the ability to verify that the data being shared are accurate and that they have not been tampered with, and the ability to track the movement of data between different entities in the system. Blockchain-based technologies can be used to provide a transparent and tamper-proof record of all data transactions in the system, making it easier to verify the actions of each entity and ensure that the data are being shared in a secure and trustworthy manner. As a result, trust and transparency are critical issues in B-IoT, and will play a key role in the success of any system that involves the sharing of data between different entities. By using blockchain-based technologies and other security measures, it is possible to establish trust and transparency in B-IoT and ensure that the system is secure, trustworthy, and effective.

7.4 Governance and regulation

The governance and regulation of B-IoT are a complex issue, because they involve many stakeholders, including governments, private organizations, and individuals. One of the main challenges is developing a regulatory framework that protects the rights and interests of all parties while fostering innovation and growth in the sector. Governments play a critical role in regulating B-IoT, because they are responsible for creating and enforcing laws and regulations that protect public safety and data security such as GDPR (Haque et al., 2021) and promote economic growth. However, the lack of global standards for B-IoT creates challenges for governments, because regulations that work in one country may not be suitable in another. Additionally, the rapidly evolving nature of B-IoT means that regulations must be agile and adaptable to keep up with technological developments. Another challenge in governance and regulation of B-IoT is the issue of data ownership and control. Because B-IoT devices generate massive amounts of

data, the question of who owns and controls those data becomes paramount. Governments must balance the rights of individuals to control their personal data with the economic benefits of sharing those data for research and development purposes. Finally, there is the issue of cybersecurity in B-IoT. The interconnected nature of B-IoT devices means that a single security breach can have far-reaching consequences. Governments must develop regulations that require B-IoT manufacturers to prioritize cybersecurity in the design and development of their devices. In conclusion, governance and regulation of B-IoT are a complex issue that requires a collaborative effort among governments, private organizations, and individuals. A regulatory framework that protects the rights and interests of all parties while fostering innovation and growth in the sector is essential for the continued development and success of B-IoT.

8 Limitations and future research directions

8.1 Limitations

This study relies on theoretical frameworks, simulations, and limited experimental data, which may not fully capture the complexities and nuances of real-world implementations. Thus, it is crucial to validate the findings and proposed solutions through extensive empirical studies, field trials, and real-world deployments.

Additionally, the rapid evolution of both blockchain and IoT technologies means that the landscape is constantly changing. New advancements, protocols, and standards may emerge which can impact the findings and recommendations of this study. Continuous monitoring and adaptation to emerging trends and technologies are necessary to ensure the relevance and applicability of the research outcomes.

Furthermore, the study may be influenced by certain assumptions and constraints specific to the chosen research methodology or context. These limitations should be carefully considered when interpreting the results and applying the findings to different scenarios or domains.

Finally, the research may not provide an exhaustive evaluation of the economic, social, and ethical implications of implementing blockchain in IoT systems. Future studies should explore the broader implications and potential challenges related to governance, legal frameworks, data privacy, and the socio-economic impact of B-IoT solutions.

Acknowledging and addressing these limitations will contribute to the advancement of knowledge and guide future research in the field of B-IoT, leading to more robust and comprehensive solutions for the challenges faced in practice.

8.2 Future research directions

As blockchain technology continues to evolve and the IoT expands its reach, there are several promising research directions that can further enhance the integration and application of blockchain in IoT systems. These future research directions aim to address the existing challenges and explore new opportunities for leveraging blockchain to improve the security, scalability, and efficiency of IoT networks.

1. Scalability solutions. One of the primary challenges in implementing blockchain in IoT is the scalability issue. Future research should focus on developing novel consensus algorithms, sharding techniques, and off-chain solutions to improve the scalability of blockchain in IoT systems. This includes exploring methods to reduce the computational and storage requirements, enabling efficient processing of a large number of IoT transactions, and ensuring timely and reliable data processing. Technological developments such as serverless computing (Gill, 2021) can also be explored to optimize resource allocation and improve scalability in B-IoT networks.

2. Privacy and data protection. Because IoT devices generate and exchange vast amounts of sensitive data, privacy and data protection become critical concerns. Future research should explore privacy-enhancing techniques such as zero-knowledge proofs, secure multi-party computation, and homomorphic encryption to ensure the confidentiality and integrity of IoT data stored on the blockchain. Additionally, developing efficient and privacy-preserving identity management systems for IoT devices can further enhance data protection.

3. Interoperability and standardization. Achieving seamless interoperability among different IoT devices and blockchain networks is crucial for widespread adoption. Future research should focus on developing

standards and protocols that enable interoperability among different blockchain platforms and IoT devices. This includes the development of cross-chain communication protocols, standardized data formats, and interoperable smart contract frameworks. Technological advancements like serverless computing can also contribute to improving interoperability by enabling dynamic and flexible integration of IoT devices and blockchain networks (Gill, 2021).

4. Energy efficiency. IoT devices are often resource-constrained and operate on limited energy sources. Future research should explore energy-efficient consensus algorithms, optimization techniques, and resource allocation strategies to minimize the energy consumption of B-IoT systems. This includes investigating the use of low-power consensus mechanisms, dynamic energy management approaches, and energy harvesting technologies. Incorporating serverless computing can also enhance energy efficiency by leveraging on-demand resource allocation and scaling capabilities (Gill, 2021).

5. Trust and governance. Blockchain introduces decentralized trust models, but challenges remain in ensuring trustworthiness and governance in IoT ecosystems. Future research should explore mechanisms for establishing trust among IoT devices and stakeholders, and develop decentralized governance models for decision-making and conflict resolution within B-IoT networks.

6. Integration with AI and ML. The integration of blockchain with AI and ML techniques presents new opportunities for IoT applications (Golec et al., 2022). Future research should explore the use of AI and ML algorithms for data analytics, anomaly detection, and predictive maintenance in blockchain-enabled IoT systems. Additionally, investigating the integration of AI-based smart contracts and autonomous agents can further enhance the automation and efficiency of IoT transactions.

7. Real-world deployment and case studies. Although blockchain technology has shown promise in IoT, real-world deployment and case studies are still limited. Future research should focus on conducting large-scale experiments, pilot projects, and field trials to validate the effectiveness and practicality of B-IoT solutions. This includes evaluating the performance, scalability, security, and usability of blockchain in diverse IoT use cases such as smart cities, healthcare, supply chain management, and energy systems. Technological developments like serverless computing can play a role in facilitating the practical deployment and implementation of B-IoT solutions (Gill, 2021).

In conclusion, future research in blockchain for IoT should aim to address the scalability, privacy, interoperability, energy efficiency, trust, integration with AI, and real-world deployment challenges. By exploring these research directions, we can unlock the full potential of blockchain technology in revolutionizing the IoT landscape and enabling secure and efficient decentralized IoT applications.

9 Conclusions

This article discusses the integration of blockchain and IoT as a solution to address the security and privacy concerns in IoT systems. It describes the concept and emergence of blockchain, mathematical models, and countermeasures for B-IoT security. The article also highlights the multi-layered architecture of B-IoT, along with smart contracts, decentralized control, immutable data storage, IAM, and consensus mechanisms as blockchain-based security solutions. It covers scalability issues, security vulnerabilities, convergence challenges, privacy and data protection issues, ownership and control of data issues, trust and transparency issues, and governance and regulation issues in B-IoT. Furthermore, the article explores the applications of B-IoT in various fields, such as smart cities and transportation, energy and utilities, healthcare and assisted living, and supply chain management. Finally, the article provides several examples of B-IoT systems specified using unified modeling language (UML), including a traffic management system, smart grid management system, remote patient monitoring system, and inventory management system.

The integration of blockchain and IoT offers immense potential for enhancing security and privacy in various domains, including smart cities, healthcare, and supply chain management. However, there are several challenges and future research directions that need to be addressed to fully realize the potential of B-IoT. One of the key challenges is scalability, because the current blockchain technology may not be

able to handle the vast amounts of data generated by IoT devices. Additionally, there is a need for more efficient consensus mechanisms to reduce the computational overheads and speed up the transactions on the blockchain. Another challenge is the lack of standardization and interoperability among different blockchain platforms and IoT devices. This can create compatibility issues and hinder the seamless integration of B-IoT solutions. Moreover, there are several legal, regulatory, and ethical challenges associated with B-IoT, including data ownership, control, and privacy. The governance and regulation of B-IoT systems need to be carefully designed to ensure transparency, accountability, and user consent.

Future research directions include exploring new consensus mechanisms, developing lightweight blockchain solutions optimized for IoT devices, and designing secure and privacy-preserving smart contracts. Moreover, the development of standards and protocols for B-IoT systems can enhance interoperability and facilitate the adoption of these solutions in various domains. Overall, B-IoT is a rapidly evolving field with enormous potential for enhancing security, privacy, and efficiency in various domains. Addressing the challenges and pursuing future research directions can enable the development of robust, secure, and scalable B-IoT solutions.

Contributors

All the authors designed the research. Sanjay MISRA and Rytis MASKELIŪNAS collected the data. Robertas DAMAŠEVIČIUS, Sanjay MISRA, and Rytis MASKELIŪNAS drafted the paper. Anand NAYYAR helped organize the paper. All the authors revised and finalized the paper.

Conflict of interest

All the authors declare that they have no conflict of interest.

References

Abdelmaboud A, Ahmed AIA, Abaker M, et al., 2022. Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges and future research directions. *Electronics*, 11(4):630. https://doi.org/10.3390/ELECTRONICS11040630

Abed S, Jaffal R, Mohd BJ, 2023. A review on blockchain and IoT integration from energy, security and hardware perspectives. *Wirel Pers Commun*, 129(3):2079-2122. https://doi.org/10.1007/s11277-023-10226-5

Akinbi A, MacDermott Á, Ismael AM, 2022. A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models. *Forens Sci Int Digit Invest*, 42-43:301470. https://doi.org/10.1016/J.FSIDI.2022.301470

Alam S, Shuaib M, Ahmad S, et al., 2022. Blockchain-based solutions supporting reliable healthcare for fog computing and Internet of Medical Things (IoMT) integration. *Sustainability*, 14(22):15312. https://doi.org/10.3390/SU142215312

Alam T, 2022. Blockchain cities: the futuristic cities driven by blockchain, big data and Internet of Things. *GeoJournal*, 87(6):5383-5412. https://doi.org/10.1007/s10708-021-10508-0

Alam T, 2023. Blockchain-based Internet of Things: review, current trends, applications, and future challenges. *Computers*, 12(1):6. https://doi.org/10.3390/computers12010006

Alharbi A, Alosaimi W, Alyami H, et al., 2021. Botnet attack detection using local global best bat algorithm for industrial Internet of Things. *Electronics*, 10(11):1341. https://doi.org/10.3390/ELECTRONICS10111341

Ali MH, Jaber MM, Abd SK, et al., 2022. Threat analysis and distributed denial of service (DDoS) attack recognition in the Internet of Things (IoT). *Electronics*, 11(3):494. https://doi.org/10.3390/ELECTRONICS11030494

Alkhateeb A, Catal C, Kar G, et al., 2022. Hybrid blockchain platforms for the Internet of Things (IoT): a systematic literature review. *Sensors*, 22(4):1304. https://doi.org/10.3390/s22041304

Altaf A, Iqbal F, Latif R, et al., 2023. A survey of blockchain technology: architecture, applied domains, platforms, and security threats. *Soc Sci Comput Rev*, 41(5):1941-1962. https://doi.org/10.1177/08944393221110148

Alzoubi YI, Al-Ahmad A, Kahtan H, et al., 2022. Internet of Things and blockchain integration: security, privacy, technical, and design challenges. *Future Int*, 14(7):216. https://doi.org/10.3390/FI14070216

Arias-Aranda D, Molina LM, Stantchev V, 2021. Integration of Internet of Things and blockchain to increase humanitarian aid supply chains performance. *Dyna*, 96(6):653-658. https://doi.org/10.6036/10067

Aslan B, Ataşen K, 2021. COVID-19 information sharing with blockchain. *Inform Technol Contr*, 50(4):674-685. https://doi.org/10.5755/j01.itc.50.4.29064

Atlam HF, Azad MA, Alzahrani AG, et al., 2020. A review of blockchain in Internet of Things and AI. *Big Data Cogn Comput*, 4(4):28. https://doi.org/10.3390/BDCC4040028

Bada AO, Damianou A, Angelopoulos CM, et al., 2021. Towards a green blockchain: a review of consensus mechanisms and their energy consumption. Proc 17th Int Conf on Distributed Computing in Sensor Systems, p.503-511. https://doi.org/10.1109/DCOSS52077.2021.00083

Bagga P, Das AK, Chamola V, et al., 2022. Blockchain-envisioned access control for Internet of Things applications: a comprehensive survey and future directions. *Telecommun Syst*, 81(1):125-173. https://doi.org/10.1007/s11235-022-00938-7

Bamakan SMH, Motavali A, Bondarti AB, 2020. A survey of blockchain consensus algorithms performance evaluation

criteria. *Expert Syst Appl*, 154:113385. https://doi.org/10.1016/j.eswa.2020.113385

Bhattacharya S, Victor N, Chengoden R, et al., 2022. Blockchain for Internet of Underwater Things: state-of-the-art, applications, challenges, and future directions. *Sustainability*, 14(23):15659. https://doi.org/10.3390/SU142315659

Bigini G, Freschi V, Lattanzi E, 2020. A review on blockchain for the Internet of Medical Things: definitions, challenges, applications, and vision. *Future Int*, 12(12):208. https://doi.org/10.3390/fi12120208

Biswas A, Wang HC, 2023. Autonomous vehicles enabled by the integration of IoT, edge intelligence, 5G, and blockchain. *Sensors*, 23(4):1963. https://doi.org/10.3390/s23041963

Bublitz FM, Oetomo A, Sahu KS, et al., 2019. Disruptive technologies for environment and health research: an overview of artificial intelligence, blockchain, and Internet of Things. *Int J Environ Res Public Health*, 16(20):3847. https://doi.org/10.3390/ijerph16203847

Butun I, Österberg P, 2021. A review of distributed access control for blockchain systems towards securing the Internet of Things. *IEEE Access*, 9:5428-5441. https://doi.org/10.1109/ACCESS.2020.3047902

Chauhan H, Gupta D, Gupta S, et al., 2021. Blockchain enabled transparent and anti-counterfeiting supply of COVID-19 vaccine vials. *Vaccines*, 9(11):1239. https://doi.org/10.3390/VACCINES9111239

Chen F, Xiao Z, Cui LZ, et al., 2020. Blockchain for Internet of Things applications: a review and open issues. *J Netw Comput Appl*, 172:102839. https://doi.org/10.1016/j.jnca.2020.102839

Čolaković A, Hadžialić M, 2018. Internet of Things (IoT): a review of enabling technologies, challenges, and open research issues. *Comput Netw*, 144:17-39. https://doi.org/10.1016/j.comnet.2018.07.017

Conoscenti M, Vetrò A, De Martin JC, 2016. Blockchain for the Internet of Things: a systematic literature review. Proc IEEE/ACS 13th Int Conf of Computer Systems and Applications, p.1-6. https://doi.org/10.1109/AICCSA.2016.7945805

Darbandi M, Al-Khafaji HMR, Hosseini Nasab SH, et al., 2022. Blockchain systems in embedded Internet of Things: systematic literature review, challenges analysis, and future direction suggestions. *Electronics*, 11(23):4020. https://doi.org/10.3390/electronics11234020

Deepika KM, Sanjay HA, Mohan MMK, 2022. Blockchain-based decentralized security using crypto-proof of stake for securing sensitive personal health care records. *Adv Eng Softw*, 173:103235. https://doi.org/10.1016/j.advengsoft.2022.103235

Doyle J, Golec M, Gill SS, 2022. BlockchainBus: a lightweight framework for secure virtual machine migration in cloud federations using blockchain. *Secur Privacy*, 5(2): e197. https://doi.org/10.1002/SPY2.197

Dziembowski S, Faust S, Kolmogorov V, et al., 2015. Proofs of space. Proc 35th Annual Cryptology Conf, p.585-605. https://doi.org/10.1007/978-3-662-48000-7_29

Elghaish F, Hosseini MR, Matarneh S, et al., 2021. Blockchain and the 'Internet of Things' for the construction industry: research trends and opportunities. *Autom Constr*, 132:103942. https://doi.org/10.1016/j.autcon.2021.103942

El-Masri M, Hussain EMA, 2021. Blockchain as a mean to secure Internet of Things ecosystems—a systematic literature review. *J Enterp Inform Manage*, 34(5):1371-1405. https://doi.org/10.1108/JEIM-12-2020-0533

Fernández-Caramés TM, Fraga-Lamas P, 2018. A review on the use of blockchain for the Internet of Things. *IEEE Access*, 6:32979-33001. https://doi.org/10.1109/ACCESS.2018.2842685

Ferrag MA, Shu L, 2021. The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: a tutorial. *IEEE Int Things J*, 8(24): 17236-17260. https://doi.org/10.1109/JIOT.2021.3078072

Florea AI, Anghel I, Cioara T, 2022. A review of blockchain technology applications in ambient assisted living. *Future Int*, 14(5):150. https://doi.org/10.3390/FI14050150

Ghosh PK, Chakraborty A, Hasan M, et al., 2023. Blockchain application in healthcare systems: a review. *Systems*, 11(1): 38. https://doi.org/10.3390/systems11010038

Gill SS, 2021. Quantum and blockchain based serverless edge computing: a vision, model, new trends and future directions. *Int Technol Lett*, 7(1):e275. https://doi.org/10.1002/itl2.275

Gill SS, Tuli S, Xu MX, et al., 2019. Transformative effects of IoT, blockchain and artificial intelligence on cloud computing: evolution, vision, trends and open challenges. *Int Things*, 8:100118. https://doi.org/10.1016/j.iot.2019.100118

Golec M, Chowdhury D, Jaglan S, et al., 2022. AIBLOCK: blockchain based lightweight framework for serverless computing using AI. Proc 22nd IEEE Int Symp on Cluster, Cloud and Internet Computing, p.886-892. https://doi.org/10.1109/CCGrid54584.2022.00106

Griffin PR, Megargel A, Shankararaman VR, 2021. A decision framework for decentralized control of distributed processes: is blockchain the only solution? In: Information Resources Management Association (Ed.), Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government. IGI Global, Pennsylvania, USA, p.272-298. https://doi.org/10.4018/978-1-7998-5351-0

Grigaliunas S, Toldinas J, Venckauskas A, et al., 2021. Digital evidence object model for situation awareness and decision making in digital forensics investigation. *IEEE Intell Syst*, 36(5):39-48. https://doi.org/10.1109/MIS.2020.3020008

Gubbi J, Buyya R, Marusic S, et al., 2013. Internet of Things (IoT): a vision, architectural elements, and future directions. *Future Gener Comput Syst*, 29(7):1645-1660. https://doi.org/10.1016/j.future.2013.01.010

Haque AB, Islam AKMN, Hyrynsalmi S, et al., 2021. GDPR compliant blockchains—a systematic literature review. *IEEE Access*, 9:50593-50606. https://doi.org/10.1109/ACCESS.2021.3069877

Hussain T, Yang BL, Rahman HU, et al., 2022. Improving source location privacy in social Internet of Things using

a hybrid phantom routing technique. *Comput Secur*, 123: 102917. https://doi.org/10.1016/j.cose.2022.102917

Kashyap V, Kumar A, Kumar A, et al., 2022. A systematic survey on fog and IoT driven healthcare: open challenges and research issues. *Electronics*, 11(17):2668. https://doi.org/10.3390/electronics11172668

Krichen M, Ammi M, Mihoub A, et al., 2022. Blockchain for modern applications: a survey. *Sensors*, 22(14):5274. https://doi.org/10.3390/s22145274

Kshetri N, 2017. Can blockchain strengthen the Internet of Things? *IT Professional*, 19(4):68-72. https://doi.org/10.1109/MITP.2017.3051335

Kumar M, Kavita, Verma S, et al., 2022a. ANAF-IoMT: a novel architectural framework for IoMT-enabled smart healthcare system by enhancing security based on RECC-VC. *IEEE Trans Ind Inform*, 18(12):8936-8943. https://doi.org/10.1109/TII.2022.3181614

Kumar M, Mukherjee P, Verma S, et al., 2022b. BBNSF: blockchain-based novel secure framework using RP^2-RSA and ASR-ANN technique for IoT enabled healthcare systems. *Sensors*, 22(23):9448. https://doi.org/10.3390/s22239448

Kumar RL, Khan F, Kadry S, et al., 2022. A survey on blockchain for industrial Internet of Things. *Alexandria Eng J*, 61(8):6001-6022. https://doi.org/10.1016/j.aej.2021.11.023

Leng JW, Chen ZY, Huang ZQ, et al., 2022. Secure blockchain middleware for decentralized IIoT towards industry 5.0: a review of architecture, enablers, challenges, and directions. *Machines*, 10(10):858. https://doi.org/10.3390/machines10100858

Li J, Herdem MS, Nathwani J, et al., 2023. Methods and applications for artificial intelligence, big data, Internet of Things, and blockchain in smart energy management. *Energy AI*, 11:100208. https://doi.org/10.1016/j.egyai.2022.100208

Li M, Pei P, Sun EC, et al., 2021. Empower artificial intelligence and blockchain to Internet of Things: development and prospect. *J Beijing Univ Technol*, 47(5):520-529 (in Chinese). https://doi.org/10.11936/bjutxb2020120020

Maroufi M, Abdolee R, Tazekand BM, 2019. On the convergence of blockchain and Internet of Things (IoT) technologies. *J Strat Innov Sustainab*, 14(1):101-119. https://doi.org/10.33423/jsis.v14i1.990

Murthy CVNUB, Shri ML, Kadry S, et al., 2020. Blockchain based cloud computing: architecture and research challenges. *IEEE Access*, 8:205190-205205. https://doi.org/10.1109/ACCESS.2020.3036812

Nyangaresi VO, Abduljabbar ZA, Mutlaq KAA, et al., 2022. Energy efficient dynamic symmetric key based protocol for secure traffic exchanges in smart homes. *Appl Sci*, 12(24): 12688. https://doi.org/10.3390/app122412688

Ogundokun RO, Arowolo MO, Misra S, et al., 2022a. An efficient blockchain-based IoT system using improved KNN machine learning classifier. In: De D, Bhattacharyya S, Rodrigues JJPC (Eds.), Blockchain Based Internet of Things. Springer, Singapore, p.171-180. https://doi.org/10.1007/978-981-16-9260-4_7

Ogundokun RO, Misra S, Maskeliunas R, et al., 2022b. A review on federated learning and machine learning approaches: categorization, application areas, and blockchain technology. *Information*, 13(5):263. https://doi.org/10.3390/INFO13050263

Pradhan NR, Singh AP, Verma S, et al., 2022a. A blockchain based lightweight peer-to-peer energy trading framework for secured high throughput micro-transactions. *Sci Rep*, 12(1):14523. https://doi.org/10.1038/s41598-022-18603-z

Pradhan NR, Singh AP, Verma S, et al., 2022b. A novel blockchain-based healthcare system design and performance benchmarking on a multi-hosted testbed. *Sensors*, 22(9): 3449. https://doi.org/10.3390/s22093449

Praveen SP, Srinivasu PN, Shafi J, et al., 2022. ResNet-32 and FastAI for diagnoses of ductal carcinoma from 2D tissue slides. *Sci Rep*, 12(1):20804. https://doi.org/10.1038/S41598-022-25089-2

Rahman S, Islam A, Uddin A, et al., 2022. A survey of blockchain-based IoT eHealthcare: applications, research issues, and challenges. *Int Things*, 19:100551. https://doi.org/10.1016/J.IOT.2022.100551

Rahmani MKI, Shuaib M, Alam S, et al., 2022. Blockchain-based trust management framework for cloud computing-based Internet of Medical Things (IoMT): a systematic review. *Comput Intell Neurosci*, 2022:9766844. https://doi.org/10.1155/2022/9766844

Ratta P, Kaur A, Sharma S, et al., 2021. Application of blockchain and Internet of Things in healthcare and medical sector: applications, challenges, and future perspectives. *J Food Quality*, 2021:7608296. https://doi.org/10.1155/2021/7608296

Ren YJ, Zhu FJ, Qi J, et al., 2019. Identity management and access control based on blockchain under edge computing for the industrial Internet of Things. *Appl Sci*, 9(10): 2058. https://doi.org/10.3390/app9102058

Saba T, Rehman A, Haseeb K, et al., 2022. Sustainable data-driven secured optimization using dynamic programming for green Internet of Things. *Sensors*, 22(20):7876. https://doi.org/10.3390/S22207876

Sedlmeir J, Buhl HU, Fridgen G, et al., 2020. The energy consumption of blockchain technology: beyond myth. *Bus Inform Syst Eng*, 62(6):599-608. https://doi.org/10.1007/s12599-020-00656-x

Shah Z, Ullah I, Li HL, et al., 2022. Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): a survey. *Sensors*, 22(3):1094. https://doi.org/10.3390/S22031094

Shi JS, Li R, 2019. Survey of blockchain access control in Internet of Things. *J Softw*, 30(6):1632-1648 (in Chinese). https://doi.org/10.13328/j.cnki.jos.005740

Singh R, Kukreja D, Sharma DK, 2023. Blockchain-enabled access control to prevent cyber attacks in IoT: systematic literature review. *Front Big Data*, 5:1081770. https://doi.org/10.3389/FDATA.2022.1081770

Srinivasu PN, Bhoi AK, Nayak SR, et al., 2021. Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network. *Electronics*, 10(12):1437. https://doi.org/10.3390/ELECTRONICS10121437

Sunny FA, Hajek P, Munk M, et al., 2022. A systematic review of blockchain applications. *IEEE Access*, 10:59155-59177. https://doi.org/10.1109/ACCESS.2022.3179690

Taherdoost H, 2023. Blockchain-based Internet of Medical Things. *Appl Sci*, 13(3):1287. https://doi.org/10.3390/app13031287

Tanwar S, Gupta N, Iwendi C, et al., 2022. Next generation IoT and blockchain integration. *J Sens*, 2022:9077348. https://doi.org/10.1155/2022/9077348

Torky M, Hassanein AE, 2020. Integrating blockchain and the Internet of Things in precision agriculture: analysis, opportunities, and challenges. *Comput Electron Agric*, 178:105476. https://doi.org/10.1016/j.compag.2020.105476

Tran NK, Babar MA, Boan J, 2021. Integrating blockchain and Internet of Things systems: a systematic review on objectives and designs. *J Netw Comput Appl*, 173:102844. https://doi.org/10.1016/j.jnca.2020.102844

Venčkauskas A, Morkevicius N, Bagdonas K, et al., 2018. A lightweight protocol for secure video streaming. *Sensors*, 18(5):1554. https://doi.org/10.3390/s18051554

Viriyasitavat W, Anuphaptrirong T, Hoonsopon D, 2019. When blockchain meets Internet of Things: characteristics, challenges, and business opportunities. *J Ind Inform Integr*, 15:21-28. https://doi.org/10.1016/j.jii.2019.05.002

Vračar LM, Stojanović MD, Stanimirović AS, et al., 2019. Influence of encryption algorithms on power consumption in energy harvesting systems. *J Sens*, 2019:8520562. https://doi.org/10.1155/2019/8520562

Vulli A, Srinivasu PN, Sashank MSK, et al., 2022. Fine-tuned DenseNet-169 for breast cancer metastasis prediction using FastAI and 1-cycle policy. *Sensors*, 22(8):2988. https://doi.org/10.3390/s22082988

Wadhwa S, Rani S, Kavita, et al., 2022. Energy efficient consensus approach of blockchain for IoT networks with edge computing. *Sensors*, 22(10):3733. https://doi.org/10.3390/S22103733

Wang WB, Hoang DT, Hu PZ, et al., 2019. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access*, 7:22328-22370. https://doi.org/10.1109/ACCESS.2019.2896108

Wang X, Yu GS, Zha X, et al., 2019a. Capacity of blockchain based Internet-of-Things: testbed and analysis. *Int Things*, 8:100109. https://doi.org/10.1016/j.iot.2019.100109

Wang X, Zha X, Ni W, et al., 2019b. Survey on blockchain for Internet of Things. *Comput Commun*, 136:10-29. https://doi.org/10.1016/j.comcom.2019.01.006

Xiong F, Xu C, Ren W, et al., 2022. A blockchain-based edge collaborative detection scheme for construction Internet of Things. *Autom Constr*, 134:104066. https://doi.org/10.1016/J.AUTCON.2021.104066

Yunana K, Alfa AA, Misra S, et al., 2021. Internet of Things: applications, adoptions and components—a conceptual overview. Proc 20th Int Conf on Hybrid Intelligent Systems, p.494-504. https://doi.org/10.1007/978-3-030-73050-5_50

Zaman U, Imran, Mehmood F, et al., 2022. Towards secure and intelligent Internet of Health Things: a survey of enabling technologies and applications. *Electronics*, 11(12):1893. https://doi.org/10.3390/ELECTRONICS11121893

Zhang WH, Qamar F, Abdali TAN, et al., 2023. Blockchain technology: security issues, healthcare applications, challenges and future trends. *Electronics*, 12(3):546. https://doi.org/10.3390/ELECTRONICS12030546

Zhao WJ, 2019. Blockchain technology: development and prospects. *Natl Sci Rev*, 6(2):369-373. https://doi.org/10.1093/nsr/nwy133

Zheng ZB, Xie SA, Dai HN, et al., 2017. An overview of blockchain technology: architecture, consensus, and future trends. Proc IEEE Int Congress on Big Data, p.557-564. https://doi.org/10.1109/BigDataCongress.2017.85

Zheng ZB, Xie SA, Dai HN, et al., 2020. An overview on smart contracts: challenges, advances and platforms. *Future Gener Comput Syst*, 105:475-491. https://doi.org/10.1016/j.future.2019.12.019

Zubaydi HD, Varga P, Molnár S, 2023. Leveraging blockchain technology for ensuring security and privacy aspects in Internet of Things: a systematic literature review. *Sensors*, 23(2):788. https://doi.org/10.3390/S23020788