network

MDPI

Article

IoT and Blockchain Integration: Applications, Opportunities, and Challenges

Naresh Adhikari [1,*] and Mahalingam Ramkumar [2]

[1] Department of Computer Science, Slippery Rock University, Slippery Rock, PA 16057, USA
[2] Computer Science & Engineering, Mississippi State University, Starkville, MS 39762, USA
* Correspondence: naresh.adhikari@sru.edu

Abstract: During the recent decade, two variants of evolving computing networks have augmented the Internet: (i) The Internet of Things (IoT) and (ii) Blockchain Network(s) (BCNs). The IoT is a network of heterogeneous digital devices embedded with sensors and software for various automation and monitoring purposes. A Blockchain Network is a broadcast network of computing nodes provisioned for validating digital transactions and recording the "well-formed" transactions in a unique data storage called a blockchain ledger. The power of a blockchain network is that (ideally) every node maintains its own copy of the ledger and takes part in validating the transactions. Integrating IoT and BCNs brings promising applications in many areas, including education, health, finance, agriculture, industry, and the environment. However, the complex, dynamic and heterogeneous computing and communication needs of IoT technologies, optionally integrated by blockchain technologies (if mandated), draw several challenges on scaling, interoperability, and security goals. In recent years, numerous models integrating IoT with blockchain networks have been proposed, tested, and deployed for businesses. Numerous studies are underway to uncover the applications of IoT and Blockchain technology. However, a close look reveals that very few applications successfully cater to the security needs of an enterprise. Needless to say, it makes less sense to integrate blockchain technology with an existing IoT that can serve the security need of an enterprise. In this article, we investigate several frameworks for IoT operations, the applicability of integrating them with blockchain technology, and due security considerations that the security personnel must make during the deployment and operations of IoT and BCN. Furthermore, we discuss the underlying security concerns and recommendations for blockchain-integrated IoT networks.

Keywords: Internet of Thing(s); blockchain network; blockchain; Cybersecurity; privacy; integrity; smart city; smart home; IoT and blockchain

Citation: Adhikari, N.; Ramkumar, M. IoT and Blockchain Integration: Applications, Opportunities, and Challenges. *Network* **2023**, *3*, 115–141. https://doi.org/10.3390/network3010006

Academic Editors: Michele Mastroianni and Francesco Palmieri

Received: 7 August 2022
Revised: 13 January 2023
Accepted: 19 January 2023
Published: 24 January 2023

1. Introduction

With the advent of the world wide web (WWW) by Tim Berners-Lee in 1989, the Internet morphed into an integral part of most life affairs, including education, communication, and business worldwide. Technologies such as a webcam—a small device to capture pictures—connected to the Internet have been evolving. The expansion of the Internet also gave way to new computing paradigms, such as the Internet of Things (IoT) and cloud computing. These two technologies have revolutionized the personal computing that began in the late 1970s (https://www.britannica.com/technology/personal-computer (accessed on 14 June 2022)). The Trojan Room coffee pot–the first webcam connected to the Internet – can be considered an earlier instance of the IoT. Today, smartwatches and hearing aids, among others, are popular IoT technologies. Similar technologies such as radio-frequency identification (RFID), and embedded electronic measuring devices such as thermostats, pressure gauges, glucose sensors, electrocardiography (EKG), electroencephalography (EEG), and sonar sensors, among others, saw their compelling applications when connected to the Internet. The actual term "internet of Things", however, was coined

in 1999 by Kevin Ashthon during his work at Procter & Gamble (https://bit.ly/2K5hUgH (accessed on 25 July 2022)). The term eventually captured widespread attention in the following decades.

IoT gained momentum in real-time sensing, effective information exchange, reduced cost and energy, and improved work efficiency/productivity. In 2008, the International Business Machines Corporation (IBM) introduced the concept of a "Smart Planet". It intends to employ massive IoTs to harvest IoT's benefits [1]. A similar concept of "smart city" is about the use of IoT to automate operations (for example, sensing, automating, and monitoring) around public facilities such as buildings, public transit systems (including buses, subways, light rail, commuter rail, trolleys, and ferries), streets installations (lamps, traffic lights, notice boards, billboards), hospitals, schools, public offices, among others inside the city premises [2]. An integral part of a "smart city" is the "smart home", which is about controlling and monitoring home appliances for audio, video, lighting, cooking, cooling, heating, surveillance, freezing, and power, among others [1] through the Internet applications.

The idea of integrating IoT has been expanding to the areas of self-driving technologies (SDTs). Google, for instance, ventured into developing self-driving technology (SDT) at the Google X lab in 2009. In 2020, Alibaba-funded start-up—AutoX—launched fully driverless RoboTaxi in Shanghai, China (https://bbc.in/3iVFCmc (accessed on 14 June 2022)). Researchers are striving to enhance the safety and effectiveness of driverless technologies to operate in complex, dynamic environments. During the recent decade, IoT has been increasingly adopted in personal and public health [2,3], home [4], agriculture and forestry [5–7], climate and meteorological studies [8], among others. In Section 3, we will briefly discuss IoT applications grouped into seven different categories of IoT systems. In the following section, let us briefly discuss the motivation and contribution of this article.

Motivation and Contribution

According to IoT Analytics (https://bit.ly/3XPS99p (accessed on 30 December 2022)), the number of IoT devices grew by 9% to reach 12.3 B globally in 2021. The COVID-19 pandemic catalyzed IoT adoption in the workplace, education, and public services. It also reported that the predicted number of connected IoT devices will reach 27B by 2025. By 2025, IoT will produce (estimated) 79.4 zettabytes (ZB) (~79×10^{12} GB) of data. By the same year, the economic impact of IoT will reach (estimated) 11 trillion dollars (https://bit.ly/3iXjRCy (accessed on 14 June 2022)). In the meantime, 58% of cyberattacks occurred over IoT devices. Those attacks mainly were DDoS attacks and pilfering of confidential data. More than 1.5 B security breaches occurred over IoT in 2021 alone. While 64% global organizations use one or more IoT solutions, 43% do not protect them adequately (https://bit.ly/3D4vQoP (accessed on 14 May 2022)).

The extent of growth and adoption of IoT is astounding. According to Cybersecurity Ventures, global cybercrime expected costs to grow by 15 percent per year over the next five years, reaching USD 10.5 trillion annually by 2025, up from $3 trillion in 2015 (https://bit.ly/3iT3sPz (accessed on 14 June 2022)). According to IBM data breach report 2021 (https://ibm.co/3XMOrxv (accessed on 15 June 2022)), the average total cost of a data breach increased by nearly 10% ($3.86 M in 2020, $4.24 M in 2021) year over year, the most significant single-year cost increase in the last seven years. However, due to a deficiency of security knowledge applicable during deploying the IoT, harvesting data from IoT, and consuming the IoT data or services, the fate of the life and properties are at higher stake than ever [9].

On the other hand, blockchain technology [10–12], yet another popular technology that operates on top of the Internet , has been adopted as a revolutionary technology for "trustless" transaction verification and process automation. Popular blockchain frameworks such as Bitcoin [13] and Ethereum [14] have been increasingly utilized for payment for online transactions and transferring money between user accounts without the need for participating banks or credit card companies. It also tracks food, prescription drugs, and

airline engine parts. As per Gartner (https://bit.ly/3HlZacF (accessed on 25 July 2022)), the value of blockchain would be 3.1 trillion in business by 2030.

In light of evolving technologies such as IoT and blockchain, this paper draws together the notion of IoT ecosystems and their existing and potential integration with blockchain technologies. This paper will discuss the overall desired security assurances in explaining the security challenges of two emerging technologies. Specifically, this paper:

1. precisely defines and exemplifies IoT, blockchain technology-related, and relevant security terminologies.
2. examines the importance of IoT and Blockchain security as evolving technologies.
3. explains the challenges of IoT and Blockchain integration.

The rest of the paper is structured as follows: In Section 2, we discuss the general architecture of an IoT network. Section 3 discusses the major applications of IoT. Section 4 exemplifies the types and applications of blockchain networks. Section 5 outlines the research methodologies. Section 6 explains the security assurances applicable to the IoT. The same section discusses the security threats of IoT. In Section 7, we explore the integration of IoT and blockchain technology. Section 8 discusses the significant challenges of IoT and blockchain integration. Section 9 discusses the ways we can address the challenges of IoT and blockchain integration. We conclude the paper with a conclusion and an outlook in Section 10.

2. Architecture of IoT

Several previous works discuss the architecture of IoT systems. Bayılmış et al. [15] discuss a six-layer IoT protocol stack. An article by Lao et al. [16] explains three- and five-layered architecture. Ray [17] examines IoT architectures for domains such as health care, smart society, and security. There are other efforts from commercial and standardization bodies to define and describe IoT architectures. For instance, the Industrial Internet Reference Architecture (IIRA) was jointly proposed by AT&T, Cisco, General Electric, IBM, and Intel [9]. The IoT-A FP7 project produced the Internet of Things Architecture(IoT-A) proposed the Reference Architecture (IIRA) (2017). The International Standardization Organization (ISO) proposed the ISO Internet of Things Reference Architecture (IoT RA—ISO/IEC WD 30141) in 2018. The IEEE P2413 WG proposed the IEEE Standard for an Architectural Framework for the Internet of Things [18]. This work, however, outlines simple four-layered IoT network architecture as depicted in Figure 1 (Left).

2.1. Sensor Layer

The sensor layer is composed of sensors and/or actuators. Sensors (or actuators) are low-powered, resource-constrained sensing and acting devices. Figure 2 shows the internal components of a sensor. Each sensor is uniquely identified by its ID or IEEE/MAC addresses. They may be connected with high-powered devices known as a relay or coordinate devices. A network of sensor devices forms a sensor network that may utilize low-power sensor network protocols such as radio-frequency identification (RFID), near field communication (NFC), ZigBee, 802.14, ANT, Bluetooth, among others [16,17].

Sensor layers may contain one or more special devices called routers in the gateway layer. Routers help extend network coverage, avoid network obstacles, and provide routes in case of network congestion or device failure. They may be connected to the network coordinator and other routers. However, in a distributed sensor network, there may be more than one network coordinator responsible for adding child nodes and authenticating them. The topology of a sensor network in sensor layers may be (i) star, (ii) mesh, and (iii) hybrid network [19].

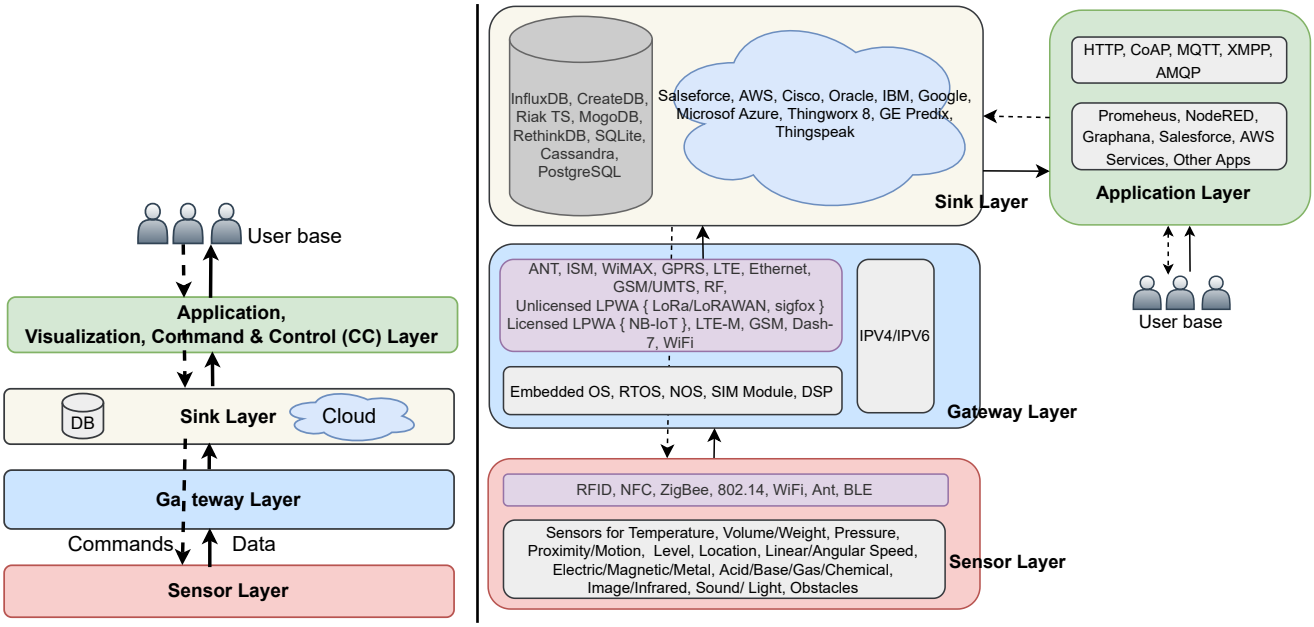

Figure 1. (**Left**) The general architecture of an IoT system consists of four major layers. The user commands and data from sensors become exchanged through the gateway layer. (**Right**) Popular instances of devices, protocols, or services in each layer of an IoT network. Discussion of the protocols and services is out of the scope of this article.

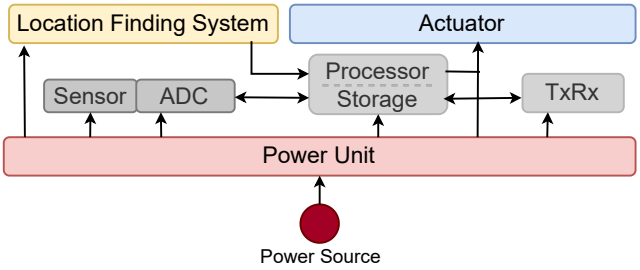

Figure 2. Major internal components of a sensor or an actuator. The component ADC stands for analog-to-digital converter, which converts an analog signal to a digital signal and vice-versa. TxRx stands for transceiver, which transmits and receives data from processor storage.

2.2. Gateway Layer

In a typical IoT ecosystem, the gateway layer consists of the particular devices responsible for registering sensor nodes, authenticating nodes, broadcasting commands, and receiving, and aggregating data from the sensors [20,21]. These devices may relay data to cloud storage engines. In a Zigbee protocol [18], for example, specific nodes known as ZigBee coordinators function in the gateway layer. Because the devices in this layer operate to bridge the external sink layer with the sensor layer, this layer is also called the bridge layer. In this layer, the devices such as embedded operating systems (OS) and real-time OS, among others, operate using diverse communication standards such as Global System for Mobile Communications (GSM/2G), Universal Mobile Telecommunications System (UMTS/3G), RF, LoRA, ANT, ISM, WiMAX, WiFi, Sigfox, Ethernet, among others [17]. The gateway devices may connect to the Internet using network-layer protocols such as IPV4 or IPV6.

2.3. IoT Sink Layer

The sink layer provides services such as storing data, encryption, decryption, data format standardization, data processing, and service management to various applications (clients) specific to the business and industry [18]. The storage devices/services may be

located locally close to the gateway layer or in the cloud containing cloud storage engines (https://bit.ly/3D5eqbC (accessed on 30 December 2022)) (for example, Amazon AWS, Google, Dropbox, Alibaba, Tencent, etc.) and data exchange services. Some popular onsite storage engines for IoT data are InfluxDB, CreateDB, Riak TS, MongoDB, RethinkDB, and Cassandra, among other (https://www.intuz.com/guide-on-top-iot-databases (accessed on 11 July 2022)).

2.4. IoT Application, Visualization, Command, and Control Layer

This layer of an IoT is an abstraction of services required for monitoring IoT devices, visualization, and analysis of IoT data, as well as command and control of IoT devices in the Sensor layer, among others. It may provide Application Programming Interfaces (APIs) to retrieve IoT data and send commands to IoT devices for business operations. IoT application layer protocols (https://bit.ly/3J5zGSh (accessed on 10 July 2022)) depend on several factors, such as data latency, reliability, and bandwidth, among others. Some of the popular application layer protocols specific to IoT systems are Message Queue Telemetry Transport (MQTT), Extensible Message and Presence Protocol (XMPP), Advanced Message Queuing Protocol (AMQP), Representational State Transfer (REST), Constrained Application Protocol (CoAP), Simple or Streaming Text Oriented Message Protocol (STOMP), Simple Media Control Protocol (SMCP), Simple Object Access Protocol (SOAP), among others [15,18].

3. Applications and Categories of IoTs

IoT has been utilized in various areas, from home to health, education, and agriculture industries. As an introduction, we highlighted the coarse evolutionary events of IoTs and different use cases. However, in this section, we instantiate major applications of IoTs under seven categories.

(1) Climate and Environmental (Aquatic/Terrestrial) IoT: Environmental IoTs are composed of sensors employed for different purposes, such as detecting pathogens, chemicals, gas, temperature, and(or) other variables in an environment, such as land or water bodies [21]. For instance, regulatory bodies such as Environment Protection Agency (EPA) often employ IoT to monitor the risk factors that affect human and environmental health. Similarly, industries based on land and water resources have benefited from the IoTs for various business needs. For instance, climate and environmental IoTs have been used for real-time monitoring and forecasting of weather, and climatic conditions in an area [8].

(2) Forest and Agricultural IoT: Applying IoTs has proved profitable in forestry, and crop/animal farming [5,22,23]. Chiefly, IoT systems have been used for managing and monitoring several aspects of farming, such as irrigation, pest control, weed control, and crop density monitoring, among others.

(3) Industrial IoT: The use of IoTs has been profitable in industries of varying kinds, such as hospitals [2], manufacturing industries, and retail and whole-shale markets, among others. Everyday use cases of an industrial IoT include remote condition monitoring, digital work instructions, predictive mainteisce, and disaster management. Using industrial IoTs brings several benefits, such as maximizing revenue, reducing time to market, and lowering operational costs.

(4) Smart Home IoT An IoT find(s) is one of its most popular applications inside a home setting. Automating lighting, sound, and kitchen work such as cooking and washing are automated by using different connected devices. Controlling and maintaining home climate can also be performed effectively using sensors such as thermostats [1,4,21].

(5) Wearable IoT: Wearable IoT comprises wearable technologies such as Fitbit, Holter monitor, personal alarm devices, smartwatches, etc. The sensing devices have become so small that they have been integrated into normal clothing items such as bras or vests, caps, shoes, and travel/school backpacks [21,24,25]. Wearable IoT has helped monitor personal health and supports remote health services [3].

(6) Smart City IoT: Smart city IoTs are an extended version of the smart home IoT [1]. It comprises many sensor technologies to sense an urban environment, streets, highways, traffic, and vehicle mobility. Smart retail shopping, intelligent health services, and smart parking are also an integral part of a smart city (https://en.wikipedia.org/wiki/Smart_city (accessed on 22 July 2022)) [4].

(7) Vehicular IoT: Vehicular IoT can be considered one of the components of a smart city IoT. Sensors that collect data from terrestrial and aerial vehicular devices constitute vehicular IoT. The data may be helpful to route the vehicular devices efficiently or may be helpful to collect environmental data such as temperature and humidity. For instance, United Parcel Service (UPS), a shipping company, deploys sensors in its transport vehicles to collect data such as mileage, speed, fuel cost, etc., for big data analysis [26,27]. Unmanned aerial vehicles (UAVs) also use different sensor data to optimize their route and operations to support "collaborative autonomous driving, and advanced transportation [28]".

4. Blockchain Technology

It is imperative to comprehend the components of the technology to understand the value that blockchain technology brings to the realm of IoT ecosystems. The major components of blockchain technology are (i) blockchain, (ii) blockchain networks, and (iii) distributed consensus mechanism [16]. In this section, we explain the working principle of blockchain technology and the types and features of blockchain networks.

4.1. Overview of Blockchain Network

As the name suggests, a blockchain network (BCN) [29] is a broad-cast network of computing nodes that maintain a copy of a synchronized storage known as a blockchain ledger. The nodes in a blockchain network operate to persistently maintain data consistency through resistance to retrospective alteration, operation transparency through network consensus, and user privacy through anonymity, among others [16].

In previous works such as [20,30,31], a blockchain is described as an "immutable" ledger"–a series of data/record blocks. Every new block in a blockchain contains a cryptographic reference to the previous block, and so on. Figure 3 shows a simple structure of a block, blockchain, and a blockchain network [30]. In a blockchain network, every new node in the network is a computing platform with storage. Generally, each node in a BCN should maintain its copy of such a ledger. A new block, however, is appended to an existing ledger only after executing a "well-formed" transaction(s). A transaction (TXN) is a data structure representing an atomic operation that involves input values and, upon execution, produces an output and changes the state of a system. The term "transaction" is frequently misused in the literature on a blockchain network. Technically, a transaction is an atomic operation whose successful execution changes the system's state. For example, consider a transaction statement: *"Transfer of monetary value x from Alice's wallet W_A to Bob's wallet W_B"*. Before the transaction is executed, the system state is $S_0 : [W_A = v_1, W_B = v_2]$. After the transaction is verified (that is, $BALANCE(W_A) - x >= 0$ is true), then the state of the system changes to $S_1 : [W_A = v_1 - x, W_B = v_2 + x]$, on the other hand, a query such as *"Balance(W_A)"* returns the balance in Alice's wallet is just similar to seeking information from storage. Usually, a query by itself does not change the system's state.and reaches an agreement on the transaction output among the network nodes. The mechanism that allows network nodes to reach an agreement on a transaction output is a consensus algorithm. Popular blockchains such as Bitcoin and Ethereum use the proof of work (PoW) consensus mechanism [13,14,32]. There are several other consensus mechanisms, such as Byzantine fault tolerance, proof of stake (PoS), proof of capacity (PoC), proof of authority, and proof of importance, among others. However, the PoW mechanism is more energy intensive and costly than other energy-efficient mechanisms such as PoS and PoC [30].

Contrary to Wang et al. [20], blockchain data storage does not prevent forging and tampering with the data; it serves as a deterrence against such activity. However, when implementing blockchain in a decentralized network environment, one can achieve a higher level of data recovery services.

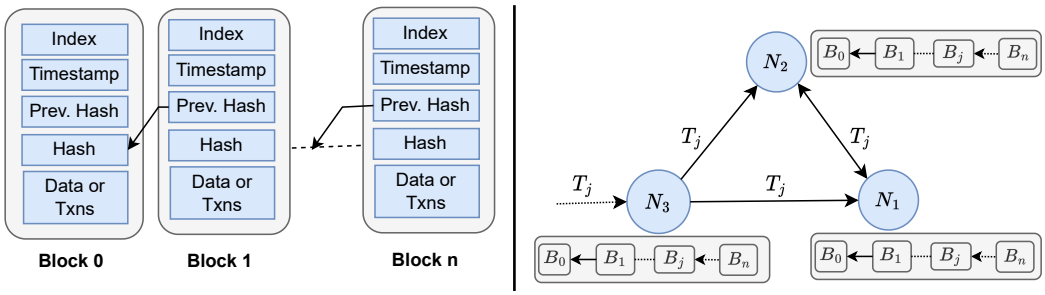

Figure 3. (**Left**) Structure of a blockchain (ledger) as a sequence of data blocks Block 0, Block 1, and so forth. Each block is linked to the previous block through a reference known as block hash, which is an output of a cryptographic function of the content of the previous block. (**Right**) A simple blockchain network with three nodes N_1, N_2, and N_3, each keeping a copy of a blockchain. As a transaction (T_j) is received by a node (N_2), it is broadcast to other nodes for execution.

4.2. Types of Blockchain Networks

Depending upon who can join a network, blockchain networks are of mainly four categories [30]: (i) public, (ii) private, (iii) consortium, and (iv) hybrid BCN.

In public, open, or global blockchain network, any node can join, leave, and perform tasks independently following the network protocol. For instance, Bitcoin and Ethereum networks are popular public blockchain networks. However, in private BCN, also called permissioned BCN, only the permitted nodes can join the network. The network manager or owner performs the node authentication and access control operations. The identity of permitted nodes is also managed as part of the network operation. Consortium BCN is a particular type of private BCN where every participant in the network is a member of the same company or organization or a group of collaborating companies or organizations. A hybrid BCN combines the feature of both public and private BCN. They provide data privacy by allowing only permitted nodes to join the network while using the public node's consensus to validate transactions that do not contain private data. Hybrid BCN is suitable for IoT systems such as supply chain management for data protection and access control [16].

In general, a blockchain network consists of two types of computing nodes, viz., verifier and normal nodes. Verifier nodes keep a copy of the complete blockchain structure and validates the transactions. These nodes are also known as full nodes. They have higher computing and storage power. They contribute to data integrity, execute smart contracts, maintain network security, and participate in network consensus mechanisms. They communicate transactions and messages using various communication protocols such as Gossip and Kademlia [16]. Normal nodes are lighter nodes that do not require high storage and computing power. They do not store a copy of the blockchain ledger; however, they obtain partial information about the blockchain status from the full nodes. Table 1 summarizes key features of blockchain networks.

Table 1. Capabilities of a Blockchain Network. Hybrid BCN is excluded from this table as it has features from both public and private BCN.

Capability	Public BCN	Private BCN	Consortium BCN
Decentralization [1]	Yes	Yes	Yes
Distributed Computing	No	No	No
TXNs [2] Verification	Performed by all (or majority) of nodes	Random or selected node	Random or selected node
Network Participation	Open to any node	Approved by network manager	Approved by network manager
TXNs (Data) Privacy	Not protected	Not-protected	Not-protected
TXNs Traceability	Pseudo-anonymous	Traceable or Pseudo-anonymous	Traceable or Pseudo-anonymous
Data Immutability	Highly immutable	Limited	Limited
Fault Tolerance	Yes	Limited	Limited
Trustworthy Execution	Yes	No	No
Consensus Mechanism	PoW, PoS, etc.	PoW, PoS, etc.	PoW, PoS, etc.
Smart Contract	Optional (mostly supported)	Optional	Optional
Cost	TXNs execution fee	Free to the internal TXNs	Free to the internal TXNs

[1] Blockchain network is a decentralized framework because the transactions are exchanged between nodes through peer-to-peer (P2P) communication, and the task of transaction verification is not centrally controlled. [2] Acronym for a transaction.

4.3. Applications of Blockchain Technology

Blockchain technology encompasses distributed ledger and a network of computing nodes. The application of the technology goes far beyond digital currencies such as Bitcoin and Ethereum. In this section, we discuss the chief applications of the technology.

- Financial Transactions and Trusted Digital Payment:In conventional digital payments, intermediaries such as banks, finances, and credit card companies act as a trusted party between a payee and a payer for any digital transactions [33]. It involves several tasks, such as bank balance verification of the payee, transaction validation, and payment verification. However, the network automates verification and validation with blockchain-based payment systems such as Bitcoin and Ethereum. As its main advantage, it reduces intermediaries' fees and transaction completion time [30].
- Process Automation: Blockchain networks may also support "smart contracts". Smart contracts are similar to regular business contracts except for the contract rules, terms (agreements), and transactions are encoded as a computer program and are executed automatically, in real-time, on blockchain network nodes [10]. The blockchain miners validate the outputs of the execution. Smart contracts save business operation time and cost and guarantee contract compliance. They have a higher potential for automating financial payments, financial audits, online transactions, document signature and approval, supply-chain operations, and so on [10].
- E-governance: E-governance is the practice of using information communication technology to provide government services, including issuing citizenship certificates, collecting taxes, delivering social securities, conducting elections, and crowdsourcing [34,35]. Blockchain technology adds advantages to e-governance by automating most of the administrative services. Countries, including Estonia and China, have invested in research on the use of blockchain in e-governance to promote efficiency and effectiveness in the provision of public services [36,37].
- Data Redundancy: One of the chief features of a blockchain network is distributed data storage [16]. Both private and public blockchain networks enforce that the computing nodes securely keep a copy of application-related data. Any alteration of data in a store can be easily detected and recovered by importing from the network peers. For instance, DokChain (https://bit.ly/3QYRws1 (accessed on 13 July 2022)) project uses blockchain as a distributed data storage to store and process financial and clinical data.

Such application enhances data integrity, auditability, and efficiency for healthcare and other related transactions and processes.

5. Materials and Methods

This paper is a culmination of a detailed literature review from research articles and online resources relevant to the "Internet of Things", "blockchain network", "blockchain, and IoT integration". Other research articles related to the security requirements of both technologies were referred to. This section includes the research questions, study sources, search criteria, and quality evaluation adopted for this study.

5.1. Research Questions

The proposed study began by identifying the research questions (RQs) as listed in Table 2.

Table 2. Research questions and their objectives.

S.N.	Research Questions	Objectives
RQ.1	What are the security assurances of an IoT?	To explore the chief security assurances pertinent to IoT systems
RQ.2	What is the threat model of IoT?	To explore different events that pose threats to the security requirements.
RQ.3	What are the application scenarios of an IoT in isolation to new technology such as blockchain technology?	To explore applications of IoT without considering blockchain technologies.
RQ.4	What are the advantages and disadvantages that come with the integration of IoT with blockchain technology?	To discuss various integration models and their merits.
RQ.5	What are the challenges for IoT and blockchain integration?	To discuss technical and non-technical problems and challenges that need to be overcome for the successful integration of IoT and blockchain technology.

5.2. Data Sources

A wide range of study resources is required for a comprehensive study such as this. For study materials, we considered peer-reviewed journal databases such as IEEEXplore, Association for Computing Machinery (ACM) digital library, Google Scholar, ResearchGate, University Library thesis, and dissertation repositories. we also considered technical reports, conference proceedings, textbooks, patents, online blogs, and news to accumulate updated facts and figures on IoT, Blockchain, and their integration.

5.3. Search Criteria

Search terminologies considered for this study logical combination of the terms listed in Table 3. The terminologies were searched against the title or the abstract of the study materials in the data sources. While specific date ranges were not considered during the search, materials published after 2015 were highly prioritized. To execute the searches, researchers applied manual search procedures.

5.4. Quality Evaluation

We employed two significant questions to filter the search outputs to match the research objectives best.

1. Q1: Does this resource refer to both the {internet of Things, IoT} and {blockchain network, blockchain}?
2. Q2: Does this resource refer to an {challenges, application} of {internet of Things, IoT} and/or {blockchain network, blockchain}?
3. Q3: Does this resource's title, abstract, or any portion of body refer to an {application, combination, merging, issues, challenges} of {Internet of Things, IoT} and/or {blockchain network, blockchain}?

Only the affirmative answers to any of the above questions from involved researchers would result in considering the resource for the study purpose.

Table 3. Database search terminologies.

Terminologies [1]
"{Internet of Things, IoT} for Blockchain {Networks, technology }"
"Integration of {Internet of Things, IoT} and Blockchain {Networks, technology}"
"Challenges of {Internet of Things, IoT} and Blockchain {Networks, technology}"
"Issues in {Internet of Things, IoT} and Blockchain {Networks,technology} integration"
"Applications of Challenges of {Internet of Things, IoT} and Blockchain {Networks, technology}"
"Merging Challenges of {Internet of Things, IoT} and Blockchain {Networks, technology}"
"Combining Challenges of {Internet of Things, IoT} and Blockchain {Networks, technology}"
"Combination of Challenges of {Internet of Things, IoT} and Blockchain {Networks, technology}"
"{Using, Use of} Blockchain network for {health, hospitals, farm, farming, poultry, fishery}"
"{Using, Use of} Blockchain network for {agriculture, forestry, smart city, smart driving}"
"{Using, Use of} Blockchain network for {parking, war, smart grid, battle}"

[1] The terms in a {} are used independently to produce all possible, unique search terms. Each search term can be used separately for a search or can be logically ORed with other search expressions.

6. Security Assurances and IoT Threat Model

A simple IoT network consists of sensor devices, a gateway device, a data storage engine, and application services. Essential security requirements of an IoT network are anonymity, integrity, privacy, authentication, authorization, availability, and audit services [20]. This section defines and exemplifies the key security terms relevant to IoT and blockchain technology.

6.1. Definitions of Security Assurances

6.1.1. Confidentiality

Confidentiality (or, privacy) [38] of data (or a message) in a storage device (such as hard disk, RAM) or a transmission channel (such as Ethernet cable, fiber optics, radio signal) ensures that the data [is not exposed/readable]/[remains secret] to illegitimate (unauthorized) parties but the authorized owner or a valid recipient of the message. For example, if any user, say, Alice, sends a message m targeted only to another user, say, Bob, on the other side through a public channel (medium), the confidentiality of the message ensures that any intermediate party, such as Eve, cannot read the message. For instance, as mandated by law [39], an individual may wish to keep his/her personal, professional, or academic matters secret; two people exchanging electronic mails (or any digital or analog messages) wish to keep their communication secret to both of them. Data privacy [40] has been a crucial requirement in demand since the medieval period up until today's interconnected world. Several encryption algorithms such as Advanced Encryption Standards (AES), Data Encryption Standard (DES), Blowfish, Rivest-Shamir-Adleman (RSA), and Elliptic Curve Digital Signature Algorithm (ECDSA) are utilized to encrypt the data (message) to achieve data or communication confidentiality [41,42]. Figure 4 depicts the simple flow of encryption and decryption schemes. Encryption is scrambling messages (data) so that illegitimate parties cannot read the message. Two major encryption schemes are (i) symmetric encryption scheme and (ii) asymmetric encryption scheme. Under symmetric encryption schemes, both encryption and decryption operations are performed by a shared secret key. Some of the algorithms that follow symmetric encryption schemes are Advanced Encryption Standards (AES), Data Encryption Standards (DES), and Blowfish, among others [41,42]. Under asymmetric encryption schemes, two different keys are used for encryption and decryption. Each entity generates a pair of mathematically related public keys and private keys. The sender encrypts a message using the recipient's public key. The recipient with the private key for the public key used for

encryption can decrypt the message using the private key. This scheme is also called public key cryptography. Examples of algorithms based on asymmetric encryption schemes are RSA, and ECDSA, among others [41,42].

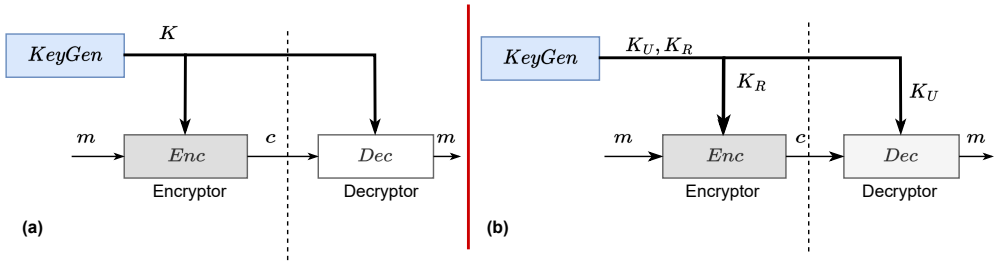

Figure 4. (**a**) A symmetric encryption scheme uses a single key, K for the encryption of a message, m and decryption of the encrypted message (cipher), c. (**b**) An asymmetric encryption scheme uses two different keys, K_U and K_R, for encryption and decryption.

6.1.2. Authentication and Authorization

Authentication is identifying legitimate human or non-human users of a system or communicating party [41,42]. It is a method that allows Bob to verify that he is communicating with Alice and not Eve. The method eventually enables Bob to verify that a message originates from Alice, not Eve.

Authorization is a mechanism by which a subject is provided with defined rights or privileges over different system resources such as files, processes, devices, etc. For example, system users such as Alice and Bob may have access rights such as read, write and execute over a file, while all other users, including Eve, may be restricted from all such operations [41].

6.1.3. Integrity

The property of message (or data) integrity [38] ensures that a message has not been tampered with or altered on its storage site or in the transfer's transit. The requirement of message integrity is essential to a wide array of digital communications, such as emails, and instant messaging, among others. For example, if Alice sends a message m to Bob, the message integrity ensures that Bob receives a message m' such that $m = m'$. In the context of IoT, data integrity ensures that the data exchanged between any two devices in an IoT network do not suffer unintentional modifications. Alteration of position, navigation, and timing of IoT sensors can severely hamper the effectiveness and trustworthiness of IoT systems.

6.1.4. Availability

The property of availability [38] guarantees that services (e.g., web server, email server, data server, telephone, power, network bandwidth, and so on) and resources (e.g., data, storage engine, computational engine) are fully available when needed or requested by their consumers such as human users, computing nodes, processes or other entities.

In the context of IoT, the availability property ensures that the components of IoT networks, such as sensor nodes, gateway servers, and data servers, among others, are available to each other and their users or owners. For instance, in an industrial IoT, temperature sensors must be available for measuring temperature throughout the operational time. In an agricultural IoT, losing equipment such as humidity and pesticide level measuring sensors, among others, can highly disrupt the production and supply chain [43]. Another issue affecting IoT data availability may arise due to the proprietary lock-in effect, where manufacturers or suppliers are forced to use outdated IoT products and services and sometimes be denied to export IoT data (https://bit.ly/3WsFfgA (accessed on 29 December 2022)).

6.1.5. Physical Security

It is related to the security assurance of availability. Physical security [18] maintains the physical integrity of computing devices, networking devices, and communication channels such as cable, twisted pair cable, fiber optics, satellite, and radio (frequency) spectrum, among others. Activities such as theft of devices and relocation of the device hamper the physical security of the device. Physical security covers hardware and software security. In the context of IoT, physical security should protect every node in each of the components of the IoT ecosystem.

6.1.6. Anonymity

Anonymizing is a task of removing explicit identifications, such as name, geo-location, address, date of birth, marital status, ethnicity, ZIP (zone improvement plan (ZIP) is a number that specifies an individual destination post office or mail delivery area.) code, SSNs (Social Security Numbers (SSN) are used to identify unique citizens in the USA. This number is used for obtaining credit, opening a bank account, claiming government benefits, and private insurance, purchase a home or a car, among others.), phone number, email address, IP address, timestamp, or any relevant attributes from the data. In the context of digital communication, the property of anonymity [44] refers to hiding users' names or relevant attributes such as date of birth, phone numbers, and emails, among others. The property of anonymity is related to an individual's privacy; however, anonymity may be achieved by removing the personally identifiable information in a data or a message. Privacy can be better preserved by anonymizing the data in transit or storage. For example, the message m may be anonymized by removing explicit information about the sender, Alice. Data without the details are of very little use to target specific user(s) and/or devices. This property prevents unstoppable surveillance of the users or computing nodes, and other analyses relevant to the person, things, or places.

6.1.7. Trustworthiness

The security of a system rests on the level of confidence one puts in security implementations and their execution. In other words, a system is secure as long as one trusts [45] its operations and outputs. For instance, we trust the secrecy of encrypted data because we have high confidence that the secret key is not exposed and the algorithm is not broken, given that it is publicly available for everyone to break. However, the "trust" in a system can be amplified by enforcing different strategies. For instance, compare the level of "trust" between an airplane with a single turbo engine and the other with two turbo engines. Given identical engines, the probability that an airplane with a single engine crashes is greater than the probability of double engines. In other words, we are improving dependability due to redundant engines. Similar is the case with the recently advancing blockchain technology, which is discussed in the following section. It is used as an infrastructure to raise trust in an output of a process being executed.

Such trust stem from the fact that the process outputs are verifiable (in terms of correctness and completeness) by all of the participating computing nodes [29,45]. The output is stored in storage whose integrity can be globally verified and backed up because multiple clones exist in physically separated locations. The other property that blockchain technology brings is fault tolerance, data security, and disaster recovery.

6.2. IoT Threat Model

With a threat modeling of an IoT ecosystem, we identify the sensitive assets, threats to those assets, and vulnerabilities that make the threats a necessary concern. Other aims are to outline security requirements, recognize security threats and vulnerabilities, quantify threat and vulnerability levels, prioritize threats and apply mitigation measures to protect the IoT-relevant assets [46].

We have several threat models [46], such as STRIDE, PASTA (https://threat-modeling.com/pasta-threat-modeling/ (accessed on 31 December 2022)), CVSS (https://ww

w.first.org/cvss/ (accessed on 31 December 2022)), attack tree, and security cards. Each of these methodologies provides different ways to access the threats faced by underlying information systems. However, because IoT technologies are evolving, the IoT may involve devices with weak device manufacturing standards, and an attack surface could be huge because of the vast network size.

In this section, we discuss a loosely coupled four-tier threat model for an IoT ecosystem as depicted in Figure 5, where an external adversary may attack devices or services on four different layers. For example, threats may occur to objects in the sensor layer. Such threats may be the theft of the sensor objects, spoofing the sensor data, and jamming the link between two sensor nodes, among others (https://bit.ly/3yYXm44 (accessed on 14 June 2022)).

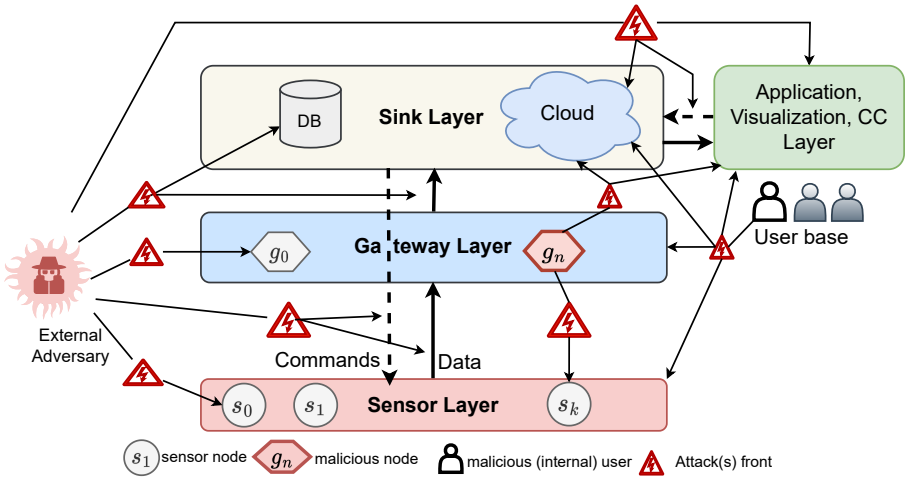

Figure 5. The threat model shows the components of the general IoT architecture and their interactions. Overall, the components and channels in an IoT form an attack surface. Three types of potential threat actors, viz., (i) external adversary, (ii) internal compromised (malicious) gateway device g_n in the gateway layer, and (iii) regular malicious (internal) user.

6.2.1. Threat and Attacks on Confidentiality

Sensitive data, including encryption keys, decision support data, and users' private information stored in an IoT node, may be stolen. For instance, in June 2019, Bitdefender (Ring Video Doorbell Pro Under the Scope, URL:https://bit.ly/3XuikD2 (accessed on 21 June 2022)) discovered a vulnerability in Amazon's Ring Video Doorbell Pro IoT camera device that permitted an attacker to physically near the device to intercept the owner's WiFi network credentials and possibly mount a more powerful attack against the home network.

Fox (https://bit.ly/3B5bWK6 (accessed on 22 June 2022)) reported that a person's smart home thermostat was hacked over WiFi to compromise the reading of the thermostat and played disturbing music from the video system. An adversary may obtain confidential sensor data causing attacks such as phishing attacks. Malicious scripts, malicious viruses/worms, Trojan horses, and malware can be exploited to steal information from IoT devices (https://bit.ly/3zpyBzq (accessed on 21 June 2022)) [27]. Attackers can utilize smart lamps, smart coffee machines, and smart speakers, among others, to steal personal information [47].

Over-the-air communication spoofing may result in the exposure of critical information shared between the nodes (https://bit.ly/3iOhwde (accessed on 1 June 2022)) [43]. Apart from directed malware attacks, the decision support applications could be implemented to steal sensitive data [43].

In industrial IoT and precision agriculture, the leak of confidential information from within an organization could cause massive damage to the supply and trust of the industries. External entities such as malicious actors, unethical domestic competitors, and foreign state and non-state adversaries could access confidential and valuable business-related,

real-time IoT data. Such access could adversely impact production, business negotiations, and trade competency, among others [43]. An example of such an attack is 'The Night Dragon' [23], where an attacker targeted and harvested a large amount of sensitive competitive proprietary operations and project-financing information from multiple oil and petrochemical companies in 2011.

6.2.2. Threat and Attacks on Availability

Several factors adversely affect the availability of an IoT network and relevant services. Loss or theft of nodes such as sensors and repeaters; jamming or interference or blocking or loss of the radio signals; disruption of the supply chain of network equipment; DDoS on the gateway devices or application servers; among others, could limit the effectiveness of an IoT network [43]. In 2015, a false data injection (FDI) cyber attack on a power grid in Ukraine resulted in the loss of service for over 22,500 customers [48]. The Mirai botnet [49] (2016) is an instance of a DoS attack where a malware named "Mirai" enslaved IoT devices such as cameras, routers, and digital video recorders to cause large-scale attacks to shut down websites and networks. Other variants of Mirai malware, such as Okiru, the Satori, the Masuta, and the PureMasuta, still live on the internet to exploit IoT devices to cause further cyber-attacks as anonymous agents (https://bit.ly/3GVt1HH (accessed on 21 June 2022)). An infected IoT device that can launch further attacks is called a bot. An IoT network of bots, also called a botnet of things, could deliver many HTTPS requests per unit of time, which can throttle a web server [23]. Attacks such as node capture attacks, malicious code injection, false data injection, replay (freshness) attacks, cryptanalysis, and side-channel attacks, sleep deprivation attacks, spoofing attacks, sinkhole attacks, wormhole attacks, man-in-the-middle, eavesdropping, and interference could adversely affect the availability of an IoT network [27].

6.2.3. Threat and Attacks on Integrity

Events such as theft of a node, unauthorized control of a node, MIM attack, insertion of a rouge sensor node, unapproved modification of input and output data, etc., may alter the integrity of data and operation of nodes in an IoT. A vital node on the sensor layer be physically stolen from the current network and may be accessed and controlled on a different network. Unauthorized node control may result from the theft of a node or an attack such as man-in-the-middle (MIM) that causes the communication between nodes to replay [12,40]. Due to an insecure channel, a MIM attack can mimic the communication and ultimately compromise the integrity of the message being exchanged between two nodes. Inserting a rouge sensor in an IoT can produce faulty data values that can negatively impact decision-making in different domains utilizing IoT [43]. Unapproved input and output data modification relevant to precision agriculture IoT, smart home, and industrial IoT, among others, can cause massive economic, environmental, and trade disruptions. Artificial intelligence and machine learning techniques have been adopted for the advanced operation of agriculture, industry, and home systems. These techniques feed on the massive data collected by an IoT. However, there is a higher risk of using insufficiently modeled algorithms, and biased predictive models for decision supports [50]. The compromised models can produce unintended and adverse effects in the current and future operations of the IoT systems [43,51].

6.2.4. Threat and Attacks on Authentication and Authorization

Password cracking is a typical attack that compromises authentic access to a network or a device such as IoT sensors. Software packages such as *aircrack-ng* (a suite of packet monitoring and injection tools available in Kali Linux oS) could be utilized to monitor and capture WiFi-protected access (WPA) handshake packets to cause dictionary attack further to crack a WiFi password. WiFi attack occurs when a malicious user tries to take control of the network by intercepting the data packets over WiFi or ZigBee channels [12]. It is a type of MIM attack that compromises the integrity of the network. An example of

such an attack is SkyJet [12]. Sontowski et al. [23] explain that other common attacks that compromise a WiFi network are evil twin access points, key reinstallation attacks, Address Resoulution Protocl (ARP) spoofing attacks, and DNS spoofing. An untrusted sensor node in a network may request sensitive data from the coordinator, and vice versa. Network nodes may enforce access control lists to manage the access of resources by participating nodes in a network.

7. IoT and Blockchain Integration

The IoT has proven to automate domestic, industrial, and business monitoring and functioning. Nevertheless, it relies on centralized cloud computing for data storage, processing, and network command and control. With the centralized model, the integrity of the data and the process output of cloud computing are always in question because IoT owners have to rely on a third party (such as cloud vendors) for the integrity of the data and the process outputs [30].

On the other hand, the basic features of a blockchain network include transparency, verifiability, data redundancy, and trustworthy [52]. These principal features can fill the gaps in providing the security-related guarantees required by an IoT network and related applications. Thus integration of an IoT and a blockchain network can serve a primary need for colossal storage, business/industry automation, fault-tolerance, and data/process integrity.

Devices in an IoT network can be designed to play different roles in a blockchain network. Edge devices such as routers, routing switches, integrated access devices, multiplexers, and gateways can be designed to store the blockchain and perform transaction validations. Intermediate devices such as relay routers can be designed to execute services for issuing transactions to a BCN on behalf of the connected resource constraint devices such as sensors. Several integration models have been discussed in previous studies [30,53]. Nevertheless, we summarize them into four major IoT and BCN integration models.

1. Sensor devices as Transaction Issuer (SaTi): In this integration model(see the interaction (a) between sensor node s and BCN in Figure 6), IoT devices such as sensors take part in issuing transactions to the external BCN. Such IoT devices should be designed to accommodate computational power and bandwidth requirements. However, the typical IoT devices do not have the storage capacity to store a complete blockchain. In many use cases, such as industrial IOTs, this model may be too costly and ineffective for sensors to communicate with an external BCN. In that case, edge devices such as IoT gateways may be employed to issue transactions on behalf of all the low-power, resource constraint IoT devices.
2. Edge devices as Transaction Issuer (EaTi): In this integration model (see the interaction (b) between edge device g and BCN in Figure 6), specially designed IoT edge devices such as gateway routers may be actively issuing transactions to an external BCN, without actually storing a copy of the blockchain ledger. This integration model is efficient, given that it requires a limited number of edge devices for interacting with the BCN.
3. Edge devices as Transaction Verifier (EaTv): This integration model extends the EaTi model, where specially designed IoT edge devices issue transactions to the BCN and maintain an entire blockchain ledger for active block validations. In many cases, edge devices could handle both issues and validate transactions being an active node for a BCN. However, unless business interests require it, an industry may not use edge devices for transaction validations, which are computationally intensive and require higher storage and bandwidth. In the figure, interaction (c) is part of this integration model.
4. Hybrid: In a hybrid integration model, IoT and blockchain interact through edge devices and specially designed IoT sensor devices. It depends on the applications whose interactions go through edge and IoT devices. In the figure, interactions (a), (b), and (c) are part of the hybrid integration model. In other words, sensor devices issue

transactions, and edge devices issue, and validate transactions for a BCN. Nonetheless, this model imposes redundancy in issuing transactions for a BCN, which is costly in terms of bandwidth.

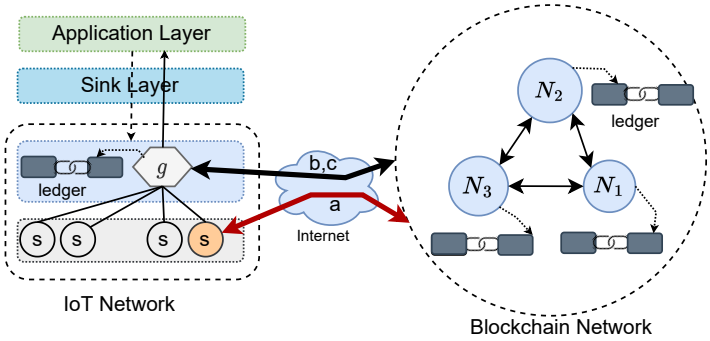

Figure 6. IoT and blockchain network integration models.

Having discussed the models of IoT and blockchain network integration, the following section discusses some compelling applications born out of IoT and blockchain integration.

7.1. Application Areas of IoT and BCN Integration

There are different challenges concerning evolving IoT. They include the problems of IoT data storage and exchange, IoT devices and user identity management, device/user authentication, and access control. With blockchain technology, well integrated with IoT, many application areas are realized for an IoT. In this section, we distinctively discuss three chief application areas of IoT-blockchain integration.

7.1.1. IoT Devices and IoT Applications' Security Enforcement

- Trust Platform: As discussed in the previous section, a blockchain network is a platform that supports transaction and process verification and public audit of the data stored in the temper-detectable blockchain ledger. Thus, the blockchain network has the potential to be used as a trusted platform for several IoT-related applications. Dedeoglu et al. [54] presented a blockchain-based trust architecture for building end-to-end trust for various IoT-based applications. Tang et al. [55] proposed a decentralized trust framework called IoT Passport for cross-platform collaborations using blockchain to enforce trusted interactions between IoT devices across platforms.
- Authentication and Access Control: Access control is a mechanism of mapping computational resources with users with appropriate access, including reading, writing, and executing. Because the blockchain network guarantees the integrity of stored data, access control mechanisms for IoT devices and applications are built and encoded on the blockchain ledger. Ji et al. [56] used an identify-based data access control model, BDAC, to provide fine-grained data access control for IoT systems. Muzammal et al. [57] proposed an enhanced authentication and access control method for IoT devices to add features, such as decentralization, secured authentication, authorization, and scalability. Zhang et al. [58] proposed an attribute-based collaborative access control scheme on top of a blockchain for IoT devices. Recently, Pal et al. [59] proposed blockchain-based IoT access control mechanisms that are claimed to provide critical features, including resource management, access rights transfer, permission enforcement, attribute management, and scalability. Košťál et al. [60] proposed using the blockchain network to manage and monitor IoT devices. Previous works from [61–63] were heavily focused on using Blockchain for IoT access control management.
- Privacy and Integrity of IoT data: Privacy and integrity are the essential properties of the IoT ecosystem. Tan et al. [64] proposed Shamir's threshold cryptography for protecting the privacy of the IoT data stored in the cloud. In this model, the end-users request decryption keys from the blockchain network to decrypt the encrypted data in the cloud. Negka et al. [65] proposed using hardware-derived functions known as

physical unclonable functions (PUFs) to detect counterfeit IoT devices. Wu et al. [66] simulated a system of assuring and detecting IoT data integrity using a distributed blockchain system. Naresh et al. [] discussed a blockchain-based method to monitor the topographic integrity of an IoT network.

7.1.2. Industrial IoT Devices and Identity Management

One of the challenges of IoT is the huge number of connected devices. Blockchain network has promising features such as decentralization and tamper-proofing of data, which could solve the issue of managing user and device identities. Nuss et al. [67] demonstrated that identity and access management could be better managed on a private blockchain for enterprise IoT devices. Vallois et al. [68] proposed distributed identity and access management for a group of industries sharing many IoT devices. They used an architecture that utilizes a blockchain network as a communication layer. Lee [69] utilized blockchain technology for identity and authentication management for mobile users and telecommunication companies. Several business startups such as ShoCard (https://www.shocard.com/en.html (accessed on 3 August 2022)), UniquID (https://uniquid.com/ (accessed on 3 August 2022)), Chronicled (htts://chronicled.com (accessed on 3 August 2022)), Riddle and Code (https://www.riddleandcode.com/ (accessed on 3 August 2022)), among others are developing blockchain-based identity verification and management platforms based on blockchain for IoT devices and users.

7.1.3. Industrial IoT Data Management and Resource Sharing/Trading

IoT produces a vast amount of highly valuable and sensitive data pertinent to industries, including healthcare, manufacturing, and supply chain management. Both the size and importance of the data demand robust ways to promote the privacy and integrity of the data. Blockchain provides vital features such as integrity and decentralization of data, thus attracting many IoT-based industries to adopt the platform for secure data management. Sigwart et al. [70] provided an IoT data provenance framework for ensuring trust in the IoT data collection, which could be used in supply chain management and health care management. El Kafhali et al. [71] presented an architecture to manage IoT data on top of blockchain and fog computing, coupled with software-defined networking (SDN) and network functions virtualization (NFV). Qing Fan et al. [72] demonstrated a comparably efficient, secure, authenticated data-sharing model for the IoT based on blockchain. Similarly, Chi et al. [73] proposed a data-sharing framework based on identity authentication and Hyberledger Fabric to ensure data-sharing security. They also proposed a community detection algorithm to segregate the data-sharing clients into different communities based on the similarity of the data label.

Mohammed et al. [74] elaborate on the use of the blockchain and e-commerce based on IoT. Jain et al. [75] discuss a decentralized distribution of solar energy between networks using IoT and blockchain networks. Khorasany et al. [76] proposed a peer-to-peer energy trading framework on blockchain to fully secure energy transactions between a pool of smart IoT devices serving energy suppliers and customers. Similarly, Bitcoin and Ethereum are popular platforms that permit payment for purchasing goods and services [13,14].

8. Challenges of IoT, Blockchain and the Integration

As an evolving technology, there are several challenges to overcome to harvest the utility of blockchain-integrated IoT fully. This section discusses significant challenges, including security, scalability, performance, and standardization of IoT and blockchain technology.

8.1. Network and Communication Security

As explained in Section 6.1, it is vital to address the security issues such as privacy, data integrity, reliability (error handling), and availability, among others. These issues are the most critical requirements for an IoT system. For example, IoT devices installed without adequate security concerns are highly prone to attacks. Such attacks can cause a high loss

of farm yield in the smart farming infrastructure not built with adequate security concerns, and end-users neglect to perform the security hardening settings [22].

Concerning blockchain, relying on blockchain to protect data privacy is far from efficient. It is because the data in a public blockchain are not generally encrypted to permit public validations [14]. Incorporating private data in a public chain makes it harder to securely share data between IoT nodes and relevant users' private data. However, if the user's anonymity is only the security goal of an organization employing an IoT, the anonymized user's data (for example, transactional data from a smart electric meter) can be provided to the public, blockchain network nodes for transaction validation. In that case, the user's unique account identity is sufficient for executing transactions [77].

8.2. Scalability

Scalability is another significant challenge to IoT as well as the blockchain network. IoT devices are easier to operate in small numbers in a local setting. However, the real-world requirements may demand the use of thousands of sensors (or actuators), which demands high-level experts to deploy and address the scalability concerns. Sensors collect very granular data values related to the environment of their deployments. It is crucial to consider the expansibility of computing power, data storage, and bandwidth, among others [78].

Concerning blockchain, regular (miner) nodes in the network require higher bandwidth, storage, and computational power. Specifically, computational power becomes more important if the blockchain network employs PoW as a consensus mechanism. Since IoT devices have minimal computational and storage capability, such nodes do not help use a blockchain network regular nodes [16]. Efforts are in progress to develop blockchain and IoT network protocols for efficient transaction validations [77]. Techniques such as off-chain transaction processing and network (or transaction or state) sharding (Sharding is the practice of segmenting an extensive network into subnets or large databases into smaller databases.) [79] techniques have been proposed and are under testing to improve the throughput of a blockchain network.

8.3. Interoperability, Standardization, Regulation, and Governance

Interoperability is a question of enabling seamless communication among heterogeneous devices. Due to device and communication varieties related to IoT, there is a lack of IoT design and communication standards. Due to the explosion of the IoT business, privacy controls, user agreements, third-party applications, and system update procedures are not uniform and consistent across platforms and applications [43]. Multitudes of standards such as IEEE, IETF, W3C, ITU-T, ONeM2M, OMG, and ETSi have been proposed for different products, services, and systems [80]. A unifying standard for cross-domain IoT communications is still far from adoption.

For example, contemporary, popular blockchain networks such as Bitcoin and Ethereum are struggling to be adopted as stable, efficient, and dependable technologies for financial transactions and health care management, among others [77]. Similarly, these technologies struggle to operate along with existing regulatory and governing bodies (https://bit.ly/3QYnLYd (accessed on 15 July 2022)).

8.4. Deployment and Detection

Due to the miniature nature of IoT devices, unscrupulous deployment has affected people's privacy. For instance, VTech, a Hong Kong-based company that produces smart and connected toys, was hacked to expose critical user information such as names, mailing addresses, and email addresses (https://bit.ly/3QYfQKH (accessed on 6 August 2022)).

As another instance, a Wi-Fi-enabled Barbie doll (https://bit.ly/3zuTmbS (accessed on 6 September 2022)) could be easily hacked to use as a surveillance tool for spying on children to listen to their conversation without their knowledge. Poachers may exploit IoT to monitor wild lives for ultimate hunting (https://bit.ly/3StPkJx (accessed on 6 August

20222)) (https://bit.ly/3BJ5h8N (accessed on 6 August 2022)). Laws prohibiting the use of IoT without transparency should be enacted to discourage the potential exploitation of IoT. Increased literacy on IoT could help encourage the ethical use of the IoT.

8.5. Performance and Resource Constraints

IoT devices are resource constraint devices [81]. They possess small memory and computational power. Additionally, they run on low power. These limitations hinder executing processes that are intensive but are required for security operations. On the other hand, a blockchain network requires validating nodes to be higher computational and storage power. For instance, according to YCharts.Com, Ethereum (https://ycharts.com/indicators/ethereum_chain_full_sync_data_size (accessed on 22 July 2022)) chain full sync data size is at a current level of 814.32 GB (22 June 2022) down from 879.18 GB one year ago, which is −7.38% from one year ago. Similarly, Bitcoin (https://ycharts.com/indicators/bitcoin_blockchain_size (accessed on 22 July 2022)) blockchain size is at a current level of 417.59 GB (22 June 2022), up from 355.57 GB one year ago, which is 17.45% from one year ago. It means there is limited opportunity for the general purpose machines to take part in transaction validations in a blockchain network [36].

8.6. Maintenance and Patching

Depending on the organizational or industrial need, IoT devices may be deployed in challenging environments such as the bottom of the sea, near the furnace, and in the forest, among others. Since IoT device firmware is not patchable, it requires reloading new images or replacing the device. Concerning the blockchain, there exists a problem with forking. A blockchain forking [79] refers to the formation of two or more versions of the blockchain due to different events such as a major protocol update, existing bug fixture, or an attack on the main blockchain protocol (https://bit.ly/3knXLJG (accessed on 15 July 2022)). All or the majority of the network should agree to the outcome of such an event. In case some wish to retain the original protocol, there occurs a fork in a blockchain. For instance, the early version of the Ethereum blockchain went through a hard fork that resulted in Ethereum Classic (ETC) in July 2016 (https://bit.ly/3Hob8mq (accessed on 21 July 2022)).

9. Meeting the IoT-BCN Challenges: Tools, Techniques and Strategies

In Section 6.1, we discussed major security assurances for an IoT network. This section discusses the tools and techniques utilized to realize the security assurances for an IoT system, a blockchain network, and their integration.

9.1. Physical Security of IoT Devices

Sensor nodes in an IoT system are often deployed in an open environment. For instance, in several IoT, such as those used for smart agriculture and forestry, smart cities, and Climate IoT, sensor nodes are installed in a public environment with no or little physical security, such as walls and boundaries. They are susceptible to physical security challenges such as theft, displacement, and physical damage. In case of displacement of the IoT nodes, the usability of the data may be negatively affected. While it may not always be feasible to create a physical boundary around IoT nodes, measures should be adopted to ensure the continuous availability of the IoT nodes. For instance, redundant IoT devices may be deployed to enhance the protections, and measures to detect physical damage, and out-of-service IoT devices should be implemented.

9.2. Confidentiality through Encryption

Encryption is a method of hiding data [38]. For enhanced confidentiality, a robust encryption algorithm such as AES that employs a 128-bit encryption key is mandated [82] for data encryption. Data in the cloud can be encrypted with the credentials of the data owners. Fine-grained data encryption in the cloud can be performed using attribute-based

encryption (ABE) as proposed by Goyal et al. [83]. It has been used on different occasions to secure data on the cloud. Studies such as [84–86] leverage a homomorphic crypto-system to encrypt locations and distance measurements harvested by such IoT. With statistical or machine learning based on IoT data, different privacy-preserving methods such as highlighted in [86–88] can be employed on IoT data. To generate machine learning models, federated machine learning models as specified by Yang et al. [89] can be employed to avoid data transfer from end devices to the remote machines. Over-the-air communication is encrypted using a secret key exchanged between the nodes.

9.3. Authentication

An essential step in securing IoT connections and data, and avoiding attacks such as spoofing and eavesdropping, is to use a secure protocol such as TLS/SSL. TLS/SSL is a cryptographic protocol for secure communication, where end devices are authenticated before initiating data exchange. Ibrahim et al. [4] applied SSL/TLS to secure intelligent home IoT while preserving the speed and agility of device and data access. Attribute-based encryption (ABE) was used for key management, and homomorphic encryption was used for data aggregation. Network authentication policies, the distribution, and the storage of encryption keys should be commissioned securely.

9.4. Anonymizing the IoT Data

IoT devices collect sensitive data such as geolocation, name, and identity of the IoT devices, among others. For example, in smart home IoT, owners of a specific home may be tied with their access to IoT devices. In forest and agricultural IoT, farmers may track the fields and the yield. Additionally, conservationists and zoological science researchers may be tracking wild-life activities (https://bit.ly/3byymJd (accessed on 8 June 2022)). What could be the repercussions if the data go into the hand of poachers? Thus, it demands highly secure and protected data harvesting and storage by such IoT. Freely available networks for anonymous connections are unreliable for two main reasons: (i) such networks are not publicly verifiable, and (ii) the Internet service providers (ISPs) may exploit their power to monitor the packets' origination and other information in insecure connections (https://bit.ly/3olJufm (accessed on 22 July 2022)). Stirapongsasuti et al. [90] demonstrated the application of *k*-anonymity method to tune the privacy of home IoT data (activities, logins, etc.) while sinking (uploading) to the remote storage. *k*-anonymity method, as proposed by Samarati et al. [44], employs the method of information (data) generalization and suppression before releasing person-specific data to safeguard the anonymity of the individuals. Other de-identification techniques include scrambling and swapping values and adding noises while retaining the result's overall statistical property [44].

9.5. Authorization

Proper authorization of IoT devices provides proper access to their users. For example, in an industry setting, mission-critical devices need to be accessible to higher privileged users such as administrators. Goyal et al. [84] demonstrated access control policies to limit the operations performed by different users on IoT devices in domestic settings. There are various types of access control mechanisms [91], such as discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), and attribute-based access control (ABAC), among others. Specially designed languages such as web ontology language (OWL) [48] have been used in formulating complex relationships between users and resources and the security policies for cloud storage and smart farming operations.

9.6. Availability

Chao et al. [26] proposed a BCN-based information exchange network for UAVs to ensure data transmission security and resilience against blocking line-of-sight. Applications can use a quieter channel and agile frequency to overcome the problem of blocking of line-of-sight of network receivers [82]. Zigbee, for instance, uses frame counters to defend

against MIM. Additionally, to protect from unauthorized control, network keys should be regularly changed [82]. It is recommended to use an intrusion detection system (IDS) for possible attacks on the system [92]. Availability can be promoted by using redundant nodes deployed for the critical IoT nodes, which operate in case the original nodes are out of service for various reasons [46]. Modern security techniques exploit artificial intelligence and machine learning to defend an IoT network, such as smart farming, smart home, and smart health, among others [23,93,94]. A system's security lies in detecting any tampering or ongoing attack on a system. Efficient intrusion detection is a framework to continuously monitor any malicious activity on an IoT network. Monshizadeh et al. [92] discussed a software-defined network with detection as a service that enables early detection of network anomalies.

9.7. Trustworthiness

As mentioned in Section 6.1.7, trustworthiness is an ultimate requirement of an information system. It can only be confirmed if other security requirements, such as privacy, integrity, and availability, are guaranteed. For instance, as IEEE Standards for Blockchain-based IoT Data Management [45] outlines, a framework of blockchain-based IoT for data management must contain a batch of trusted sensing, storage, communication, and networking to monitor any malicious activity on an IoT network continuously information system can be significantly promoted by augmenting it with a blockchain-based solution.

9.8. IoT Security Controls and Policies

As explained in Section 6, the attack surface of an IoT network is as large as the Internet. Applying the tools and techniques to provide the desired security assurances for an IoT system is insufficient. Additionally, it is crucial to establish and apply standard security controls to effectively mitigate the threats to an IoT system and thwart foreseeable attacks on the system. In this section, we adapt the CIS Controls (The Center for Internet Security (CIS) is an "independent, nonprofit organization with a mission to create confidence in the connected world" (https://www.cisecurity.org/controls (accessed 22 June 2022); Alternative to CIS's controls are the framework from National Institute of Science and Technology (NIST), ISO 27001, and PCI-DSS among others [95].)) to strengthen the protection and defend an IoT system.

- Implement IoT devices and firmware version inventory management: This control encourages network owners to create an effective inventory of authorized network and sensor devices. This inventory assists in establishing authorized network devices and detecting unauthorized devices.
- Implement IoT application services and version management: This control provides a mechanism to create an inventory of software or firmware packages used by IoT devices. Such inventory is valuable during firmware/software vulnerability fixing and patch management.
- Implement IoT network or device access control management: Access control mechanism is one of the crucial techniques to provide operational and other permissions over IoT devices. It also assists in monitoring IoT device access by different users. Proper authentication mechanisms should also be implemented to avoid leaking or reusing user credentials such as usernames and passwords.
- Implement IoT network and application isolation: It is crucial to establish a distinction between an IoT network and an application (or analysis) layer. While an IoT network is a network of devices contributing to harvesting sensor data, the application layer consists of services used by end users to support organization decisions. A stringent isolating boundary should be created to mitigate risks of vulnerabilities affecting each other.
- Implement IoT network and access Log management: This control encourages network owners to collect, alert, review and retain events logs that could assist in detecting, comprehending, and recovering from any attack on an IoT system.

- Data protection and recovery management: Critical asset produced by an IoT is the vast set of application-specific data. Implementing adequate data backup procedures is crucial to avoid data loss during an attack or a disaster. User access and data encryption should also be properly managed to prevent information leaks.

10. Discussion and Conclusions

This paper presented several topics, including the evolution of IoT things, its architecture and major application areas, security assurances of an IoT, and its relevance to blockchain technology. Blockchain technology can offer unique features such as decentralization, transparency, and data integrity to the areas of IoT to give rise to robust, compelling applications that span from home to industry to agriculture and farming. However, from our study, we concluded that the actual use case of the blockchain-integrated IoT lies in the reliable infrastructure supporting blockchain network operations. On the other hand, international standardization of the operation of devices and communication protocols is highly desirable for burgeoning use cases of the IoT.

As discussed previously, there are several ways IoT and blockchain can be integrated to harvest riveting application services. At the same time, there are myriads of threats to IoT that could not be resolved by BCN integration. For instance, BCN cannot solve common threats for an IoT, are physical tampering with the deployed IoT devices and malware injection, DDoS attacks, and battery drainage attacks, among others [96]. The seamless interactions between IoT devices and the BCN depend on several factors, including computational power and bandwidth. An issue affecting IoT data availability may arise due to the proprietary lock-in effect, where manufacturers or suppliers are forced to use potentially incompetent IoT products and services and sometimes be denied to export data (https://bit.ly/3J5hY1p (accessed on 29 December 2022)). With respect to blockchain technology, we still lack a reliable, scalable, efficient, affordable, well-governed, general-purpose blockchain platform to execute IoT-specific services. Much work is required to enhance the financial, operational reliability, and governance of popular open-source blockchain networks such as Bitcoin and Ethereum.

Author Contributions: Conceptualization, N.A.; software, N.A.; validation, M.R. formal analysis, N.A. and M.R.; investigation, N.A.; resources, N.A.; writing—original draft preparation, N.A.; writing—review and editing, M.R.; visualization, N.A.; supervision, N.A and M.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: N. Adhikari would like to thank Sam Thangiah, Chair of the Computer Science Department at Slippery Rock University, for lending tools for provisioning the IoT system(s) in the lab, and Vibha Acharya for encouraging in the research endeavors.

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

Abbreviations

The following abbreviations are used in this manuscript:

ABE	Attribute-Based Encryption
AES	Advanced Encryption Standards
BC	Blockchain
BCN	Blockchain Network
CIS	Center for Internet Security
CVSS	Common Vulnerability Scoring System
DES	Data Encryption Standard
DoS	Directory of open access journals
ECDSA	Elliptic Curve Digital Signature Algorithm
FDI	False Data Injection
IIRA	The Industrial Internet Reference Architecture

LTE-M	data
LoRa	Long Range
MAC	Mandatory Access Control
MIM	Man-in-the-Middle
NFC	Near Field Communication
OWL	Web Ontology Language
PASTA	Process for Attack Simulation and Threat Analysis
PoS	Proof of Stake
PoW	Proof of Work
RBAC	Role Based Access Control
RFID	Radio Frequency Identification
RSA	Rivest–Shamir–Adleman Algorithm
TCP	Transport Control Protocol
TLS/SSL	Transport Layer Securuirty/Socket Layer Security
TXN	Transactions (Plr. TXNs)
Temp.	Temperature
UAV	Unmanned Aerial Vehicle
WIMAX	Worldwide Interoperability for Microwave Access
WWW	World Wide Web
ZB	Zettabytes

References

1. Ainane, N.; Ouzzif, M.; Bouragba, K. Data security of smart cities. In Proceedings of the 3rd International Conference on Smart City Applications, Tetouan, Morocco, 10–11 October 2018. [CrossRef]
2. YIN, Y.; Zeng, Y.; Chen, X.; Fan, Y. The internet of things in healthcare: An overview. *J. Ind. Inf. Integr.* **2016**, *1*, 3–13. [CrossRef]
3. Arunkumar, N.; Pandimurugan, V.; Hema, M.S.; Azath, H.; Hariharasitaraman, S.; Thilagaraj, M.; Govindan, P. A Versatile and Ubiquitous IoT-Based Smart Metabolic and Immune Monitoring System. *Comput. Intell. Neurosci.* **2022**, *2022*, 9441357. [CrossRef] [PubMed]
4. Ibrahim, J.M.; Karami, A.; Jafari, F. A secure smart home using Internet-of-Things. In Proceedings of the 9th International Conference on Information Management and Engineering, Barcelona, Spain, 9–11 October 2017; pp. 69–74. [CrossRef]
5. Dineva, K.; Atanasova, T. Design of Salable IoT Architecture based on AWS for Smart Livestock. *Animal* **2021**, *11*, 2697. [CrossRef] [PubMed]
6. Sudha, M.K.; Manorama, M.; Aditi, T. Smart Agricultural Decision Support Systems for Predicting Soil Nutrition Value Using IoT and Ridge Regression. *Agris Online Pap. Econ. Inform.* **2022**, *14*, 95–106. [CrossRef]
7. Oliver, S.T.; González-Pérez, A.; Guijarro, J.H. An IoT proposal for monitoring vineyards called senviro for agriculture. In Proceedings of the 8th International Conference on the Internet of Things, IOT 2018, Santa Barbara, CA, USA, 15–18 October 2018. [CrossRef]
8. Ahire, D.B.; Gond, D.V.J.; Ahire, N.L. IoT Based Real-Time Monitoring of Meteorological Data: A Review. In Proceedings of the 3rd International Conference on Contents, Computing & Communication (ICCCC-2022), Nashik, India, 26–27 February 2022; pp. 1–12. [CrossRef]
9. Casola, V.; De Benedictis, A.; Rak, M.; Villano, U. Toward the automation of threat modeling and risk assessment in IoT systems. *Internet Things* **2019**, *7*, 100056. [CrossRef]
10. Pennino, D.; Pizzonia, M.; Vitaletti, A.; Zecchini, M. Blockchain as IoT Economy Enabler: A Review of Architectural Aspects. *J. Sens. Actuator Netw.* **2022**, *11*, 20. [CrossRef]
11. Huh, S.; Cho, S.; Kim, S. Managing IoT devices using blockchain platform. In Proceedings of the International Conference on Advanced Communication Technology, ICACT, PyeongChang, Republic of Korea, 19–22 February 2017; pp. 464–467. [CrossRef]
12. Mehta, P.; Gupta, R.; Tanwar, S. Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. *Comput. Commun.* **2020**, *151*, 518–538. [CrossRef]
13. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Technical Report. 2008. Available online: bitcoin.org (accessed on 19 September 2022).
14. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32 2019.
15. Bayılmış, C.; Ebleme, M.A.; Çavuşoğlu, Ü.; Küçük, K.; Sevin, A. A survey on communication protocols and performance evaluations for Internet of Things. *Digit. Commun. Netw.* **2022**, *8*, 1094–1104. [CrossRef]
16. Lao, L.; Li, Z.; Hou, S.; Xiao, B.; Guo, S.; Yang, Y. A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling. *ACM Comput. Surv.* **2020**, *53*, 1–32. [CrossRef]
17. Ray, P.P. A survey on Internet of Things architectures. *J. King Saud Univ. Comput. Inf. Sci.* **2018**, *30*, 291–319. [CrossRef]
18. Lea, P. *Internet of Things for Architects*, 1st ed.; Packt Publishing: Birmingham, UK, 2018; pp. 1–676.
19. Dahlberg, R.; Pulls, T.; Peeters, R. Efficient Sparse Merkle Trees Caching Strategies and Secure (Non-) Membership Proofs. *Lect. Notes Comput. Sci.* **2**016, *10014 LNCS*, 199–215. [CrossRef]

20. Wang, G.; Shi, Z.; Nixon, M.; Han, S. ChainSplitter: Towards blockchain-based industrial IoT architecture for supporting hierarchical storage. In Proceedings of the 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019, Atlanta, GA, USA, 14–17 July 2019; pp. 166–175. [CrossRef]
21. McGrath, M.J.; Scanaill, C.N. *Sensor Technologies—Healthcare, Wellness and Environmental Applications*; Apress: Berkeley, CA, USA, 2013; pp. 1–302. [CrossRef]
22. Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and Privacy in Smart Farming: Challenges and Opportunities. *IEEE Access* **2020**, *8*, 34564–34584. [CrossRef]
23. Sontowski, S.; Gupta, M.; Laya Chukkapalli, S.S.; Abdelsalam, M.; Mittal, S.; Joshi, A.; Sandhu, R. Cyber Attacks on Smart Farming Infrastructure. In Proceedings of the 2020 IEEE 6th International Conference on Collaboration and Internet Computing, CIC 2020, Virtual, 1–3 December 2020; Institute of Electrical and Electronics Engineers Inc.: Interlaken, Switzerland, 2020; pp. 135–143. [CrossRef]
24. Mann, S. Historical account of the 'WearComp' and 'WearCam' inventions developed for applications in 'personal imaging'. In Proceedings of the International Symposium on Wearable Computers, Digest of Papers, Cambridge, MA, USA, 13–14 October 1997; pp. 66–73. [CrossRef]
25. Tariq, N.; Qamar, A.; Asim, M.; Khan, F.A. Blockchain and smart healthcare security: A survey. In *Procedia Computer Science*; Elsevier: Amsterdam, The Netherlands, 2020; Volume 175, pp. 615–620. [CrossRef]
26. Chao, H.; Maheshwari, A.; Sudarsanan, V.; Tamaskar, S.; Delaurentis, D.A. UAV traffic information exchange network. In Proceedings of the 2018 Aviation Technology, Integration, and Operations Conference, Atlanta, GA, USA, 25–29 June 2018. [CrossRef]
27. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A Survey on internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE internet Things J.* **2017**, *4*, 642–646. [CrossRef]
28. Peng, C.; Wu, C.; Gao, L.; Zhang, J.; Yau, K.L.A.; Ji, Y. Blockchain for Vehicular internet of Things: Recent Advances and Open Issues. *Sensors* **2020**, *20*, 5079. [CrossRef] [PubMed]
29. Ramkumar, M.; Adhikari, N. Blockchain Based Redistricting with Public Participation. *J. Inf. Secur.* **2022**, *13*, 140–164. [CrossRef]
30. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of Blockchains in the internet of Things: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1676–1717. [CrossRef]
31. Alotaibi, B. Utilizing Blockchain to Overcome Cyber Security Concerns in the internet of Things: A Review. *IEEE Sens. J.* **2019**, *19*, 10953–10971. [CrossRef]
32. Xu, J. The Application of Blockchain Technology in Equity Incentive. *E3S Web Conf.* **2021**, *235*, 15–18. [CrossRef]
33. Vora, G. Cryptocurrencies: Are Disruptive Financial Innovations Here? *Mod. Econ.* **2015**, *06*, 816–832. [CrossRef]
34. Hou, H. The Application of Blockchain Technology in E-Government in China. In Proceedings of the 6th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 31 July–3 August 2017; Volume 235, pp. 1–4. [CrossRef]
35. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
36. Saxena, S.; Shao, D.; Nikiforova, A.; Thapliyal, R. Invoking blockchain technology in e-government services: A cybernetic perspective. *Digit. Policy Regul. Gov.* **2022**, *24*, 246–258. [CrossRef]
37. Kassen, M. Blockchain and e-government innovation: Automation of public information processes. *Inf. Syst.* **2022**, *103*, 101862. [CrossRef]
38. Stallings, W. *Cryptography and Network Security: Principles and Practice 7th Global Edition*, 7th ed.; Pearson Education Limited: Harlow, UK, 2017.
39. Tiedemann, P. The Human Right to Privacy *Philos. Found. Hum. Right* **2020**. *44*, 197–214. [CrossRef]
40. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
41. Pass, R.; Shelat, A. *A Course in Cryptography*, 3rd ed.; Printed Online 2010; pp. 1–192. Available online: https://bit.ly/3GZEiGN (accessed on 19 December 2022)
42. Bruce, S. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed.; John Wiley & Sons, Inc: New York, NY, USA, 1996.
43. Brown, A.; Bethel, G.; Koehler, S. Threats To Percision Agriculture. Technical Report, 2018. Available online: https://bit.ly/3XNsSwC (accessed on 20 October 2022)
44. Samarati, P.; Sweeney, L. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. In Proceedings of the IEEE Symposium on Research in Security and Privacy (S&P), Oakland, CA, USA, 3–6 May 1998.
45. *IEEE Std 2144.1-2020*; IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management. 2021. Institute of Electrical and Electronics Engineers Inc.: New York, USA, 2021; pp. 1–20. [CrossRef]
46. Bradbury, M.; Jhumka, A.; Watson, T.; Flores, D.; Burton, J.; Butler, M. Threat-modeling-guided Trust-based Task Offloading for Resource-constrained internet of Things. *ACM Trans. Sens. Netw.* **2022**, *18*, 1–41. [CrossRef]

47. Hilt, S.; Kropotov, V.; Mercês, F.; Rosario, M.; Sancho, D. The internet of Things in the Cybercrime Underground. Available online: https://bit.ly/2lZRnKv (accessed on 20 December 2022)
48. Chukkapalli, S.S.L.; Piplai, A.; Mittal, S.; Gupta, M.; Joshi, A. A Smart-Farming Ontology for Attribute Based Access Control. In Proceedings of the 2020 IEEE 6th Intl Conference on Big Data Security on Cloud, BigDataSecurity 2020, 2020 IEEE Intl Conference on High Performance and Smart Computing, HPSC 2020 and 2020 IEEE Intl Conference on Intelligent Data and Security, IDS 2020, Baltimore, MD, USA, 25–27 May 2020; pp. 29–34. [CrossRef]
49. Line, M.B.; Zand, A.; Stringhini, G.; Kemmerer, R. Targeted attacks against industrial control systems: Is the power industry prepared? In Proceedings of the ACM Conference on Computer and Communications Security. Association for Computing Machinery, Scottsdale, AZ, USA, 3–7 November 2014; Volume 2014, pp. 13–22. [CrossRef]
50. Nguyen, A.; Yosinski, J.; Clune, J. Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 7–12 June 2015.
51. Tyagi, T. Botnet of Things: Menace to Internet of Things. In Proceedings of the third International Conference on Computing: Communication, Network and Security (IC3NS-2018), Sikar, Rajasthan, India, 25–27 October 2018; pp. 61–65.
52. Wüst, K.; Gervais, A. Do you need a Blockchain? In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 20–22 June 2018; pp. 45–54. [CrossRef]
53. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
54. Dedeoglu, V.; Jurdak, R.; Putra, G.D.; Dorri, A.; Kanhere, S.S. A Trust Architecture for Blockchain in IoT. In Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Houston, TX, USA, 2–14 November 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 190–199. [CrossRef]
55. Tang, B.; Kang, H.; Fan, J.; Li, Q.; Sandhu, R. IoT Passport: A Blockchain-Based Trust Framework for Collaborative internet-of-Things. In Proceedings of the 24th ACM Symposium on Access Control Models and Technologies, Toronto, ON, Canada, 3–6 June 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 83–92. [CrossRef]
56. Ji, Y.; Xiao, X.; Wu, F.; Chen, F.; Liu, S. BIDAC: Blockchain-Enabled Identity-Based Data Access Control in IoT. In Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, Melbourne, Australia, 14–17 December 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 400–405. [CrossRef]
57. Muzammal, S.M.; Murugesan, R.K. Enhanced Authentication and Access Control in internet of Things: A Potential Blockchain-Based Method. *Int. J. Grid Util. Comput.* **2021**, *12*, 469–485. [CrossRef]
58. Zhang, Y.; Li, B.; Liu, B.; Wu, J.; Wang, Y.; Yang, X. An Attribute-Based Collaborative Access Control Scheme Using Blockchain for IoT Devices. *Electronics* **2020**, *9*, 285. [CrossRef]
59. Pal, S.; Dorri, A.; Jurdak, R. Blockchain for IoT access control: Recent trends and future research directions. *J. Netw. Comput. Appl.* **2022**, *203*, 103371. [CrossRef]
60. Košťál, K.; Helebrandt, P.; Belluš, M.; Ries, M.; Kotuliak, I. Management and Monitoring of IoT Devices Using Blockchain. *Sensors* **2019**, *19*, 856. [CrossRef]
61. Banerjee, S.; Bera, B.; Das, A.K.; Chattopadhyay, S.; Khan, M.K.; Rodrigues, J.J. Private blockchain-envisioned multi-authority CP-ABE-based user access control scheme in IIoT. *Comput. Commun.* **2021**, *169*, 99–113. [CrossRef]
62. Iftekhar, A.; Cui, X.; Tao, Q.; Zheng, C. Hyperledger Fabric Access Control System for internet of Things Layer in Blockchain-Based Applications. *Entropy* **2021**, *23*, 1054. [CrossRef] [PubMed]
63. Tan, L.; Shi, N.; Yu, K.; Aloqaily, M.; Jararweh, Y. A Blockchain-Empowered Access Control Framework for Smart Devices in Green internet of Things. *ACM Trans. Internet Technol.* **2021**, *21*, 80. [CrossRef]
64. Tan, L.; Yu, K.; Yang, C.; Bashir, A.K. A Blockchain-Based Shamir's Threshold Cryptography for Data Protection in Industrial internet of Things of Smart City. In Proceedings of the 1st Workshop on Artificial Intelligence and Blockchain Technologies for Smart Cities with 6G, New Orleans, LA, USA, 25–29 October 2021; Association for Computing Machinery: New York, NY, USA, 2021; pp. 13–18. [CrossRef]
65. Negka, L.; Gketsios, G.; Anagnostopoulos, N.A.; Spathoulas, G.; Kakarountas, A.; Katzenbeisser, S. Employing Blockchain and Physical Unclonable Functions for Counterfeit IoT Devices Detection. In Proceedings of the International Conference on Omni-Layer Intelligent Systems, Crete, Greece, 5–7 May 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 172–178. [CrossRef]
66. WU, X.; Kong, F.; Shi, J.; Bao, L.; Gao, F.; Li, J. A Blockchain internet of Things Data Integrity Detection Model. In Proceedings of the International Conference on Advanced Information Science and System, Singapore, 15–17 November 2019; Association for Computing Machinery: New York, NY, USA, 2019. [CrossRef]
67. Nuss, M.; Puchta, A.; Kunz, M. Towards Blockchain-Based Identity and Access Management for internet of Things in Enterprises. In *Trust, Privacy and Security in Digital Business*; Furnell, S., Mouratidis, H., Pernul, G., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 167–181.
68. Vallois, V.; Mehaoua, A.; Amziani, M. Blockchain-based Identity and Access Management in Industrial IoT Systems. In Proceedings of the 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), Bordeaux, France, 18–20 May 2021; pp. 623–627.
69. Lee, J.H. BIDaaS: Blockchain Based ID As a Service. *IEEE Access* **2018**, *6*, 2274–2278. [CrossRef]

70. Sigwart, M.; Borkowski, M.; Peise, M.; Schulte, S.; Tai, S. Blockchain-Based Data Provenance for the internet of Things. In Proceedings of the 9th International Conference on the internet of Things, Bilbao, Spain, 22–25 October 2019; Association for Computing Machinery: New York, NY, USA, 2019. [CrossRef]
71. El Kafhali, S.; Chahir, C.; Hanini, M.; Salah, K. Architecture to Manage internet of Things Data Using Blockchain and Fog Computing. In Proceedings of the 4th International Conference on Big Data and Internet of Things, Tangier-Tetuan, Morocco, 23–24 October 2019; Association for Computing Machinery: New York, NY, USA, 2019. [CrossRef]
72. Fan, Q.; Chen, J.; Deborah, L.J.; Luo, M. A secure and efficient authentication and data sharing scheme for internet of Things based on blockchain. *J. Syst. Archit.* **2021**, *117*, 102112. [CrossRef]
73. Chi, J.; Li, Y.; Huang, J.; Liu, J.; Jin, Y.; Chen, C.; Qiu, T. A secure and efficient data sharing scheme based on blockchain in industrial internet of Things. *J. Netw. Comput. Appl.* **2020**, *167*, 102710. [CrossRef]
74. Mohammed, S.; Fiaidhi, J.; Ramos, C.; Kim, T.H.; Fang, W.C.; Abdelzaher, T. Blockchain in ECommerce: A Special Issue of the ACM Transactions on internet of ThingsBlockchain in ECommerce: A Special Issue of the ACM Transactions on internet of Things. *ACM Trans. Internet Technol.* **2021**, *21*, 11–55. [CrossRef]
75. Jain, R.; Dogra, A. Solar Energy Distribution Using Blockchain and IoT Integration. In Proceedings of the 2019 International Electronics Communication Conference, Okinawa, Japan, 7–9 July 2021; Association for Computing Machinery: New York, NY, USA, 2019; pp. 118–123. [CrossRef]
76. Khorasany, M.; Dorri, A.; Razzaghi, R.; Jurdak, R. Lightweight blockchain framework for location-aware peer-to-peer energy trading. *Int. J. Electr. Power Energy Syst.* **2021**, *127*, 106610. [CrossRef]
77. Attaran, M. Blockchain technology in healthcare: Challenges and opportunities. *Int. J. Healthc. Manag.* **2022**, *15*, 70–83. [CrossRef]
78. Bataineh, M.R.; Mardini, W.; Khamayseh, Y.M.; Yassein, M.M.B. Novel and Secure Blockchain Framework for Health Applications in IoT. *IEEE Access* **2022**, *10*, 14914–14926. [CrossRef]
79. Wang, L. The Challenge and Prospect of Scalability of Blockchain Technology. In Proceedings of the 2021 5th International Conference on Computer Science and Artificial Intelligence, Beijing, China, 4–6 December 2021; pp. 296–301. [CrossRef]
80. Gazis, V. A Survey of Standards for Machine-to-Machine and the internet of Things. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 482–511. [CrossRef]
81. Bertino, E.; Sandhu, R.; Thuraisingham, B.; Ray, I.; Li, W.; Gupta, M.; Mittal, S. Security and Privacy for Emerging IoT and CPS Domains. In Proceedings of the Association for Computing Machinery (ACM), Baltimore, MD, USA, 24–27 April 2022; pp. 336–337. [CrossRef]
82. Maximizing Security in Zigbee Networks. Available online: https://bit.ly/3GVr4ed (accessed on 19 December 2022)
83. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the ACM Conference on Computer and Communications Security, Taipei, Taiwan, 21–24 March 2006; pp. 89–98. [CrossRef]
84. Goyal, G.; Lie, P.; Sural, S. Securing Smart Home IoT Systems with Attribute-Based Access Control. In Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, Baltimore, DC, USA, 27 April 2022; ACM: Baltimore, DC, USA, 2022; pp. 37–46. [CrossRef]
85. Li, M.; Yu, S.; Zheng, Y.; Ren, K.; Lou, W. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *24*, 131–143. [CrossRef]
86. Yan, Q.; Lou, J.; Vuran, M.C.; Irmak, S. Scalable Privacy-preserving Geo-distance Evaluation for Precision Agriculture IoT Systems. *ACM Trans. Sens. Netw.* **2021**, *17*, 1–30. [CrossRef]
87. Bertino, E.; Carminati, B.; Ferrari, E.; Thuraisingham, B.; Gupta, A. Selective and Authentic Third-Party Distribution of XML Documents. *IEEE Trans. Knowl. Data Eng.* **2004**, *16*, 1263–1278. [CrossRef]
88. Al-Rubaie, M.; Chang, J.M. Privacy-Preserving Machine Learning: Threats and Solutions. *IEEE Secur. Priv.* **2019**, *17*, 49–58. [CrossRef]
89. Yang, Q.; Liu, Y.; Chen, T.; Tong, Y. Federated Machine Learning: Concept and Applications. *ACM Trans. Intell. Syst. Technol.* **2019**, *10*, 1–19. [CrossRef]
90. Stirapongsasuti, S. Decision Making Support for Privacy Data Upload in Smart Home. In Proceedings of the Adjunct: Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers, London, UK, 9–13 September 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 214–217. [CrossRef]
91. Sandhu, R.S.; Samarati, P. Access Control: Principles and Practice. *IEEE Commun. Mag.* **1994**, *32*, 40–48. [CrossRef]
92. Monshizadeh, M.; Khatri, V.; Kantola, R. Detection as a service: An SDN application. In Proceedings of the International Conference on Advanced Communication Technology, ICACT, Pyeongchang, Republic of Korea, 19–22 February 2017; pp. 285–290. [CrossRef]
93. Ullah, Z.; Al-Turjman, F.; Mostarda, L.; Gagliardi, R. Applications of Artificial Intelligence and Machine learning in smart cities. *Comput. Commun.* **2020**, *154*, 313–323. [CrossRef]

94. Chukkapalli, S.S.L.; Mittal, S.; Gupta, M.; Abdelsalam, M.; Joshi, A.; Sandhu5, R.; Joshi, K. Ontologies and artificial intelligence systems for the cooperative smart farming ecosystem. *IEEE Access* **2020**, *8*, 164045–164064. [CrossRef]
95. CIS Controls Version 8. Available online: https://bit.ly/3kDgHnK (accessed on 19 December 2022)
96. Iqbal, W.; Abbas, H.; Daneshmand, M.; Rauf, B.; Bangash, Y.A. An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security. *IEEE Internet Things J.* **2020**, *7*, 10250–10276. [CrossRef]