big data and cognitive computing

MDPI

Review

A Review of Blockchain in Internet of Things and AI

Hany F. Atlam [1,2,*], Muhammad Ajmal Azad [3], Ahmed G. Alzahrani [1] and Gary Wills [1]

[1] Electronic and Computer Science Department, University of Southampton, Southampton SO17 1BJ, UK; a.g.m.alzahrani@soton.ac.uk (A.G.A.); gbw@soton.ac.uk (G.W.)
[2] Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[3] Department of Engineering and Technology, University of Derby, Derby DE22 1GB, UK; m.azad@derby.ac.uk
* Correspondence: hfa1g15@soton.ac.uk

Received: 15 September 2020; Accepted: 12 October 2020; Published: 14 October 2020

Abstract: The Internet of Things (IoT) represents a new technology that enables both virtual and physical objects to be connected and communicate with each other, and produce new digitized services that improve our quality of life. The IoT system provides several advantages, however, the current centralized architecture introduces numerous issues involving a single point of failure, security, privacy, transparency, and data integrity. These challenges are an obstacle in the way of the future developments of IoT applications. Moving the IoT into one of the distributed ledger technologies may be the correct choice to resolve these issues. Among the common and popular types of distributed ledger technologies is the blockchain. Integrating the IoT with blockchain technology can bring countless benefits. Therefore, this paper provides a comprehensive discussion of integrating the IoT system with blockchain technology. After providing the basics of the IoT system and blockchain technology, a thorough review of integrating the blockchain with the IoT system is presented by highlighting benefits of the integration and how the blockchain can resolve the issues of the IoT system. Then, the blockchain as a service for the IoT is presented to show how various features of blockchain technology can be implemented as a service for various IoT applications. This is followed by discussing the impact of integrating artificial intelligence (AI) on both IoT and blockchain. In the end, future research directions of IoT with blockchain are presented.

Keywords: Internet of Things; blockchain technology; IoT with blockchain; review; IoT and blockchain integration

1. Introduction

The Internet of Things (IoT) is a modern technology where various physical and virtual devices can be connected and communicate with each other over the Internet often without human intervention. IoT devices are mainly utilized to tackle our everyday problems and to facilitate our life by sensing and collecting various kinds of information about our surrounding physical environment that are utilized to create novel digitized services. The IoT has achieved massive success on an international scale, with billions of devices sold and utilized globally to date across many consumer markets [1].

Despite the multiple benefits introduced by the IoT system in numerous areas, the centralized IoT architecture, such that all IoT objects are linked, managed, and dominated through a central server, faces multiple challenges. These challenges are standing as a barrier in the way of future developments of IoT applications. For instance, a single point of failure, in which if the server goes down, all IoT applications and services associated with it will go down, affects the availability and quality of service provided by the IoT system [2]. Furthermore, the centralized server stores all data created form various IoT devices in one location (central server) which makes it a desirable goal for many attackers. Furthermore, preserving data privacy appears to be doubtful, as all IoT data, which involve sensitive

and personal information, are kept in one location in a remote server under the full control of a third-party provider [3]. Besides, the scalability of the centralized architecture is another problem, which may not be a practical solution for the IoT system that increases in billions every year [4].

With multiple issues introduced by the centralized IoT architecture, moving the IoT into one of the distributed ledger technologies may be the correct choice. Among the common and popular kinds of distributed ledger technologies is the blockchain. It is essentially a distributed, decentralized, shared and immutable ledger that keeps the information of various transactions that ever happened in a certain peer-to-peer (P2P) network [3]. A group of transactions were collected and assigned a block in the ledger. Each block has a timestamp and hash function which are used to link the current block to the previous block. This creates chains of blocks, which is why it is called the blockchain. To store a transaction in the distributed ledger, the majority of nodes in the blockchain network should record their agreement. Blockchain technology promotes information sharing in which all contributing users/nodes in the blockchain network have a replica of the golden/original ledger so that all users are updated with recently added transactions or blocks [5].

Integrating the IoT with blockchain brings numerous advantages. For example, employing decentralized and distributed attributes of blockchain technology can handle issues of security and a single point of failure associated with the centralized IoT architecture, as there is no need for a central server to control IoT devices and their communications with each other. Furthermore, blockchain delivers better security and privacy, since blockchain utilizes sophisticated cryptography algorithms, hash functions and timestamp, which provide a secure computing environment. In addition, the blockchain provides tamper-proof and immutable ledger to safeguard data against harmful attacks such that any data change cannot be stored in the ledger only if the majority of contributing users validate it [6]. This, in turn, delivers a trusted system where the participating IoT devices are the only objects to accept or discard a transaction based on their consent [7].

The objective of this paper was to provide a comprehensive discussion of integrating the IoT system with blockchain technology. This paper starts by presenting an overview of the IoT system involving its characteristics and centralized architecture. Then, an overview of blockchain technology is presented by highlighting its main components and features. This is followed by presenting a comprehensive review of integrating IoT with blockchain by highlighting how blockchain resolved issues of IoT, the architecture of IoT with blockchain, why blockchain platforms needed to implement IoT with blockchain and the recent studies that have outlined the convergence of IoT with blockchain. Then, blockchain as a service for the IoT is presented to show how various features of blockchain technology can be implemented as a service for various IoT applications. This is followed by discussing the impact of integrating artificial intelligence (AI) on both IoT and blockchain. In the end, future research directions of IoT with blockchain are discussed.

Compared to the existing reviews conducted on integrating IoT with blockchain, this paper provides an up-to-date comprehensive survey of IoT with blockchain. In this paper, novel and significant aspects of IoT with blockchain are discussed, such as blockchain as a service for the IoT and the impact of integrating AI on both IoT and blockchain. The related survey failed to discuss the implementation of blockchain in IoT applications. Besides, they failed to discuss implementing features of blockchain as a service for the IoT system. Furthermore, the related survey failed to highlight the need for integrating AI with IoT and blockchain, which is significant especially with the huge amount of data created by IoT devices and the scalability issues of both IoT and blockchain.

The contribution of this paper can be summarized as follows:

1. Investigating the state-of-the-art research and recent studies of IoT with blockchain;
2. Discussing the need for integrating IoT with blockchain and how blockchain resolved issues of the centralized IoT architecture;
3. Introducing blockchain as a service to deploy features of blockchain as a service for the IoT system;
4. Exploring the impact of integrating AI on both IoT and blockchain;
5. Discussing future research directions of IoT with blockchain.

The remainder of this paper is organized as follows: Section 2 provides an overview of the IoT system; Section 3 provides an overview of blockchain technology; Section 4 discusses the integration of IoT with blockchain; Section 5 introduces blockchain as a service for the IoT; Section 6 discusses the impact of integrating AI in IoT and blockchain; Section 7 presents future research directions of the IoT with blockchain; and Section 8 concludes the paper.

2. An Overview of IoT

The term IoT refers to the modern proliferation of internet-enabled devices with embedded computing capability. The term describes a wide range of technologies, from the internet-enabled security cameras and surveillance devices, networked industrial equipment and sensors to domestic products like fridges and cars. The IoT is an ever increasingly popular technology that has developed with ubiquitous computing in today's era of technology. IoT devices have helped to facilitate the way we live using IoT applications like smart homes, smart cities and smart transportation [1].

With the term IoT being so broad and widely used, there is no specific definition. The IoT was defined by several organizations and researchers. It is defined by the International Telecommunication Union (ITU) in 2012 as "*a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies*" [8].

The number of IoT objects bypassed the population worldwide in 2008. With several advantages of the IoT system, new applications and services can be established every day. According to Statista [9], the number of IoT objects is anticipated to be about 31 billion worldwide by the end of 2020. This number is expected to grow significantly to reach about 75 billion devices by the end of 2025, as depicted in Figure 1.

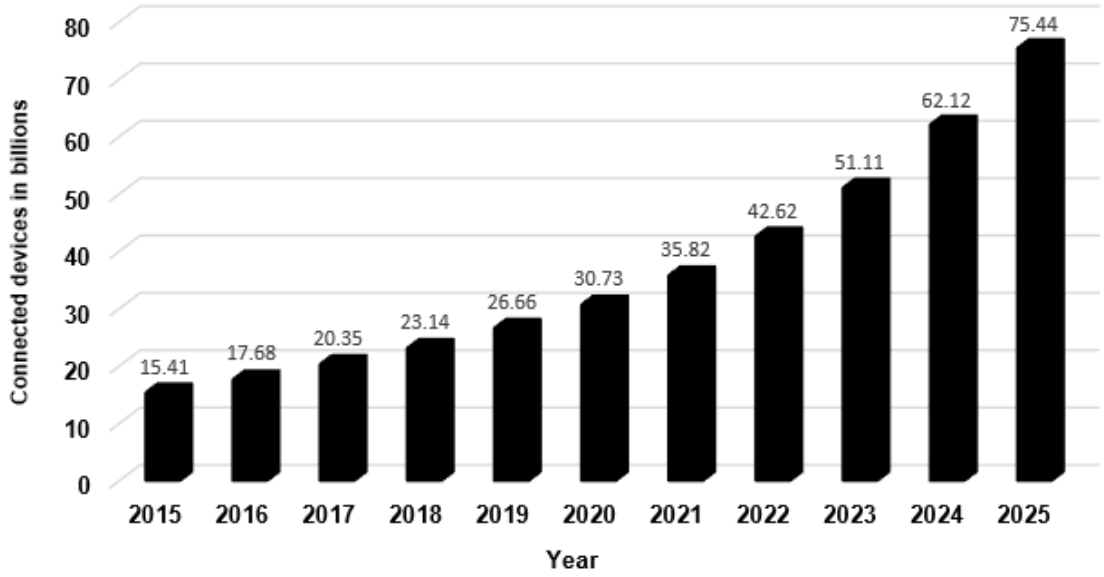

Figure 1. Expected Internet of Things (IoT) growth from 2015 to 2025 [3].

In addition, the IoT market is growing almost exponentially. According to Statista, the estimated revenue of IoT in 2015 was USD 743 billion. This number is expected to increase dramatically to reach USD 1710 billion by the end of 2019 [9].

2.1. Features of IoT System

The IoT system describes an innovative technology that can change our life, business, and economy. The IoT produces countless digitized services and applications that provide several benefits over existing solutions. These applications and services share some common features, which include [1,5,10]:

- **Sensing capabilities**: the main technology that promotes developments in various IoT domains is the wireless sensor network (WSN). WSN is typically a network of sensors that sense information about the surroundings and send this information over a communication medium for processing. Sensors are the building blocks of the IoT that enable collecting all real-time and contextual information about the surroundings which allow the decision-makers to make accurate and precise decisions on time.
- **Connectivity**: this is among the key characteristics of the IoT system that enables billions of devices and objects to be accessible remotely. Additionally, it allows various objects in our environment to be connected and communicate with each other over the Internet, which allows creating new applications and services.
- **Large scale network**: as stated earlier, the IoT system includes billions of devices that are expected to reach 75 billion devices by the end of 2025 [9]. This large number of devices and objects create a large-scale network that cannot be managed by traditional or classical methods.
- **Dynamic system**: the IoT is a dynamic system in nature. It can connect various objects in different locations. In addition, with sensors that collect various real-time and contextual information about surroundings, IoT devices can be dynamically adapted to changing circumstance and conditions.
- **Intelligence capabilities**: with advanced hardware, software and sensing capabilities that enable collecting a vast volume of contextual data, IoT devices can make smart decisions in several conditions and cooperate intelligently with other collaborating objects.
- **Big data**: there are billions of IoT devices, which creates a vast volume of data that cannot be analysed using traditional data analytics methods. This refers to the term "big data". The IoT is among the richest sources of big data that creates a vast volume of data that needs innovative analytics methods to have the full benefits of IoT data.
- **Unique identity**: the IoT system enables various objects to connect over the Internet. Having the ability to connect to the Internet can be guaranteed only if each device can have a unique identity or identifier such as the IP address. For the IoT system, manufactures give a unique identifier to each device that allows it to update devices to appropriate platforms especially in case there was a security breach. Therefore, although IoT devices are in billions, each device has a unique identity.
- **Autonomous decision**: there is many sensors in the IoT system, which enable collecting huge contextual and real-time data about the surrounding environment. These dynamic data allow IoT devices to make context-aware and autonomous decisions.
- **Heterogeneity**: the IoT system allows different devices and objects to be addressable and communicate with each other over the Internet. These devices come with heterogeneous characteristics including communication protocols, operating systems, platforms, and other software and hardware components. Despite these heterogeneous characteristics, the IoT system allows all these devices to communicate with each other efficiently and effectively.

2.2. Centralized IoT Architecture

Managing a set of nodes to work together to formulate a system needs to have a certain architecture design. Among the popular designs is the centralized architecture, which is built using a centralized server to control and manage a set of nodes. These nodes vary from an advanced computer system, laptop, mobile phone, etc., which are capable of performing various types of operations. The centralized server acts as the manager that deals with all requests coming from various nodes and manages task scheduling and allocation among nodes in the network [11]. A simple form of a centralized architecture is shown in Figure 2, where all nodes in the network are connected through a central server.

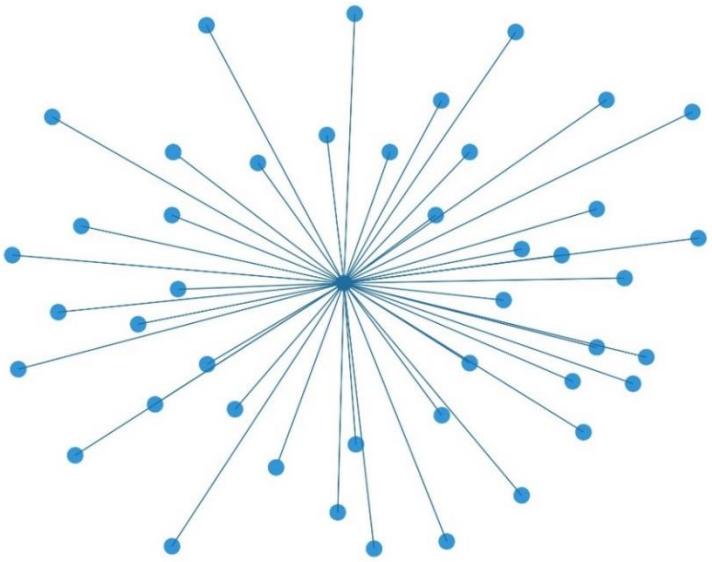

Figure 2. Centralized architecture.

The IoT system is among the common examples of a centralized system, which is also called client–server architecture. In this approach, all IoT devices and objects are connected, managed and authenticated through a centralized server, which is typically a cloud server. According to Fernández-Caramés and Fraga-Lamas [4] and Lu et al. [12], the centralized IoT architecture consists of three key layers; the perception, network and application layer, as shown in Figure 3. Although there are several centralized architecture designs for the IoT system containing four, five and six layers suggested by different researchers, this three-layer architecture shows the functionality of the IoT system smoothly and easily.

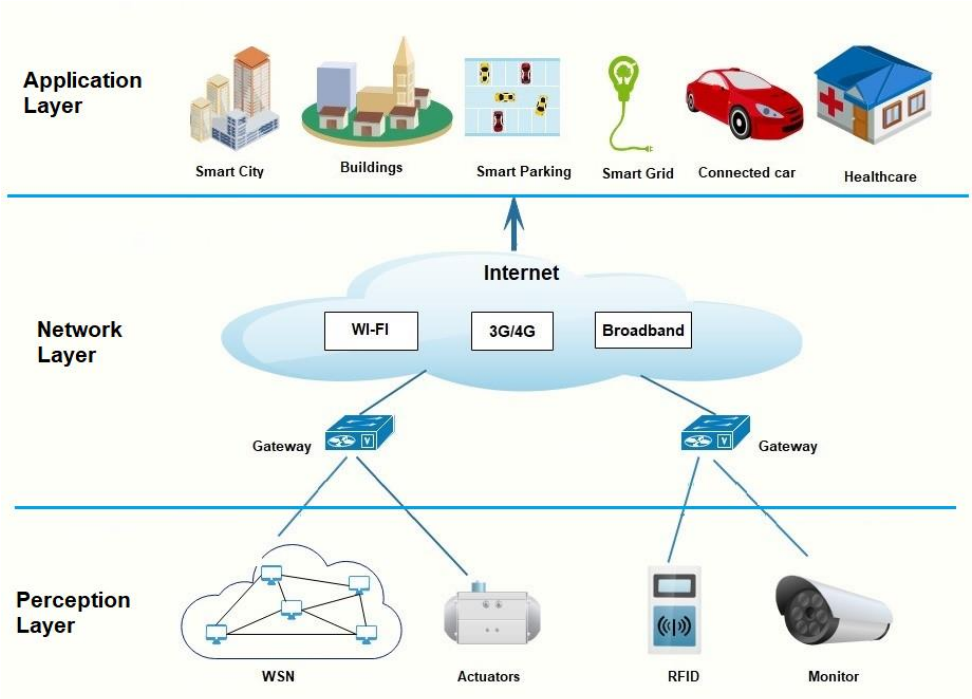

Figure 3. Three-layer architecture of the IoT system.

The first layer of the IoT architecture is the perception layer (also called the sensing layer). This layer involves various kinds of sensors, Radio Frequency Identifications (RFIDs), actuators and

WSNs. The main responsibility of this layer is to sense and perceive the surrounding environment and collect the relevant data that can be processed and extract meaningful information to understand and control our surrounding physical world [13]. Based on the collected data, IoT devices can make context-aware and autonomous decisions using actuators. The network layer is utilized to connect and communicate all IoT things and devices over the Internet, where the centralized server is located. This layer incorporates gateways that represent the communication points between the perception and network layer. Various communication technologies and protocols were employed in this layer such as 3G/4G, ZigBee, Wi-Fi, Bluetooth and Broadband to transfer the data between the perception and application layer. The application layer comprises of diverse IoT applications that utilizes huge amounts of data collected and processed at the perception and network layer, respectively, and produce digitized services in diverse domains such as healthcare, smart parking, smart home, smart city, wearables, smart grid, agriculture and many others [5,14].

The existing centralized model of the IoT system provides several advantages to connect and communicate a wide variety of devices that are managed by the centralized server. Hence, the whole charge of the IoT network is managed through a central server, which is simpler to manage and maintain. In addition, it saves costs of implementing several complete workstations of hardware and software in the network, in which most of the processing operations are only handled by the centralized server. Therefore, most nodes in the network can be like a terminal to connect to the central server. Besides, the centralized IoT architecture delivers better physical security as most IoT data are kept in a single location, which is simpler to safeguard from physical harms [5].

On the other hand, the centralized IoT architecture introduces multiple challenges. For example, it faces scalability issues as it cannot handle the constant increase in IoT devices. In addition, it introduces numerous security and privacy challenges [15]. Table 1 provides a summary of issues related to the IoT centralized architecture.

Table 1. Summary of challenges of the IoT centralized model.

Challenge	Description
Single Point of Failure	As the centralized server performs all processing operations and manages communications between various devices, this produces a single point of failure in which if the server goes down, the whole network of devices will be unreachable.
Security	Security is among the key challenges in the IoT centralized model since all data processing operations and data storage are done in one location and through a central server which makes it susceptible to different kind of threats specifically Denial of Service (DoS) [13].
Privacy	Various types of real-time data including sensitive information are collected from IoT devices such as habits, passwords, personal and financial information, etc. These collected data are kept in one location under the full control of the centralized third-party server which can violate the data privacy. Additionally, storing it in one location can make it easier to be breached [16].
Inflexibility	The centralized server controls communications and processing operations between all nodes linked to the IoT network, which creates a huge workload. To handle this workload, the centralized server plans the load to evade peak-load issues. However, this limits user flexibility while doing their own tasks due to the tight agenda and delay linked to this process [17].
Cost	The central server performs all processing and communication operations between all nodes in the network which require high hardware and software capabilities to handle this workload. Additionally, it needs huge retaining storages that are able to store data coming from various IoT devices. All these high capabilities of hardware and software come with a high cost [4].

Table 1. *Cont.*

Challenge	Description
Scalability	Among the topmost challenges associated with the centralized model is scalability. Managing and controlling all nodes in the network by a central server can scale well only in small networks. Employing the notion of a centralized system with large enterprise organizations that involve several branches in different areas will be unreasonable. The number of IoT devices is increasing constantly which means that the centralized model is unable to scale and function efficiently [18].
Access and Diversity	Among the important aspects of an efficient system is the capability to provide access to all their users with diverse needs. However, the centralized system requires its users to access the information steadily using identical processes. Furthermore, most centralized systems utilize a particular operating system for the whole network which restricts diversity within the network. For the IoT system that contains heterogeneous and diverse devices, this will produce a serious issue that requires being handled [19].

3. Blockchain Technology

The world continued utilizing the centralized architecture in which a central server is needed to control the processing and scheduling of tasks until Szabo created a decentralized digital currency at the end of 1990. Ten years later, Bitcoin cryptocurrency was offered. Blockchain became generally widespread after Satoshi Nakamoto's paper in 2009 [20]. This section presents an overview of blockchain technology.

3.1. An Overview of Blockchain

Blockchain technology is among the most recent themes that attracted the attention of several organizations and researchers due to the countless benefits it provided over existing solutions [21]. A blockchain is essentially a distributed, decentralized and immutable ledger that keeps the information of the various transactions that ever happened in a certain P2P network [22]. To store a transaction in the distributed ledger, most of the nodes should record their agreement. This requires a consensus mechanism. The most common and popular consensus mechanisms are Proof of Stake (PoS) and Proof of Work (PoW). A group of transactions are collected and assigned a block in the ledger. A timestamp and hash function associated with each block are used to link the block to the previous block. So, multiple blocks are chained together, and given the name blockchain. The hash function is mainly used to validate the integrity of the block's content or data [3]. The blockchain technology promotes information sharing in which all participating users/nodes in the blockchain network have a copy of the original ledger, so all nodes are updated with newly added transactions or blocks [5].

There are various definitions for the blockchain. For instance, Coinbase, the world's largest cryptocurrency exchange, defined blockchain as "*a distributed, public ledger that contains the history of every bitcoin transaction*" [23]. In the same way, the Oxford dictionary defines blockchain. It stated, "*a digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly*" [24]. These definitions describe the blockchain from cryptocurrency's viewpoint that does not reflect the reality that blockchain can be utilized in numerous domains. Moreover, discussing key components of blockchain, Sultan et al. [25] delivered a common description for the blockchain. It stated, "*a decentralized database containing sequential, cryptographically linked blocks of digitally signed asset transactions, governed by a consensus model*".

3.2. Components of Blockchain

Blockchain technology can deliver several benefits over existing solutions. There are a set of elementary components of the blockchain, which include ledger, block, hashing, transaction, minor and consensus mechanisms, as depicted in Figure 4. The ledger is a data structure that is utilized to store various types of information. There are significant differences between the classical database and the ledger. A database system stores data in the form of tables with columns and rows. Moreover, it uses a

relational model for querying and gathering data by connecting information from several sources [26]. On the other hand, the ledger is utilized to store all the transactions that were ever made from all participating users in the network. Additionally, the ledger was distributed among the participating nodes, so each user has its own replica of the ledger.

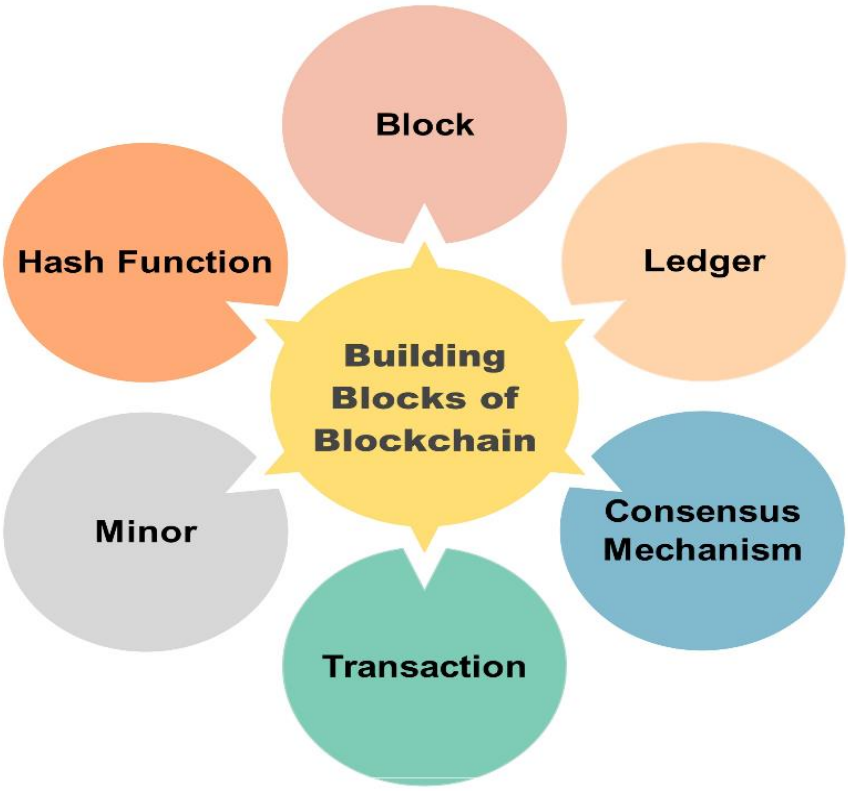

Figure 4. Main components of blockchain.

Block is among the primary components of the blockchain. Each block comprises a set of transactions. The blocks were chained together by storing a unique hash value of the preceding block in the existing block. This link blocks together like a chain. The hash function is used to validate the data integrity of the content of each block. Basically, the hash function is a mathematical problem that the minors need to crack to find a block. The reason to use the hash function is that it is collision-free in which it is very hard to create two identical hashes for two different digital data. So, assigning a hash value for each block can serve as a way to identify the block and also validate its contents [18].

A transaction is the smallest unit of process or operation in which a set of transactions are combined and stored in a block. A certain transaction cannot be added to the block unless the majority of the participating nodes in the blockchain network record their consent. The size of a transaction is important for minors as small transactions require less power and are easier to validate. Minors are computers/agents that attempt to solve a complex mathematical problem (typically, a form of hash functions) to explore a new block. Discovering a new block is started by broadcasting new transactions to all nodes, and then each node combines a set of transactions into a block and operates to discover the block's proof-of-work. If a node discovers a block, then the block will be broadcasted to all the nodes to be verified [27].

3.3. Features of Blockchain

Blockchain can deliver numerous advantages for multiple fields and applications. This new technology shares some common features that involve:

- **Decentralization**: blockchain is typically a decentralized and distributed environment that is based on the P2P communication between communicating nodes. The decentralization enables utilizing the processing power of all contributing users, which decreases latency and removes the single point of failure. This feature overcomes the single point of failure issue.
- **Transparency**: in contrast to the centralized model where the central server is only having the full control and access to all data, blockchain offers a good level of transparency in which all nodes have access to all the details of the transactions that ever happened in their network. Besides, each node has a copy of the distributed ledger to keep updated with changes. In addition, the absence of a third party increases business friendliness and trust [28].
- **Immutability**: among the crucial characteristics of blockchain is the capability of guaranteeing the transactions' integrity through producing immutable ledgers. In contrast to the centralized model where data integrity is only managed and preserved through the central authority, which can be a threat, the blockchain uses hash functions that are collision-free to link each block to the previous block which maintains the integrity of the block's contents. In addition, blocks stored in the ledger can never be changed only if most of the users confirm that change [26].
- **Better security**: among the advantages of blockchain technology is that it provides better security over existing solutions. With the use of public key infrastructure, blockchain provides a secure environment against various types of attacks. In addition, the consensus mechanism provides a trusted method that improves the security of the blockchain. Moreover, the absence of the single point of failure in the blockchain technology, that can affect the whole systems, provides better security over the centralized model [29].
- **Anonymity**: despite blockchain utilizing a ledger that is distributed between all users, blockchain provides an anonymous identity to protect the nodes' privacy. The anonymity feature can be utilized to provide a secure and private voting system [30].
- **Cost reduction**: in contrast to the centralized architecture in which the advanced and complete hardware and software system is required to build the centralized server, the blockchain technology reduces the costs related to fitting and sustaining large centralized servers as it utilizes the processing power of communicating devices [31].
- **Autonomy**: the ability to make autonomous decisions is among the features that the blockchain technology can provide. It allows the manufacturing of new devices that are able to make smart and autonomous decisions. For instance, blockchain features including tamper-proof and better security can be used to build better and secure autonomous vehicles [7].

4. IoT with Blockchain

The IoT has become one of the unprecedented technologies that enable virtual and physical objects to be linked together over the Internet, which in turn produce numerous opportunities in different domains. The unexpected development of the IoT system has unlocked innovative chances in various fields. However, the IoT still has some issues that stand like a wall in the face of the promised spreading of IoT objects. Among these issues is the lack of trust and confidence. The current IoT centralized model utilizes a third-party central authority that has complete control of data collection and processing from various IoT objects without any clear restrictions about how the collected data are being used. Hence, the central authority is like a block box for IoT users, which is a convincing situation for the majority of IoT devices' owners [32].

On the other hand, blockchain technology delivers decentralized, autonomous, trustless and distributed environment. In distinction to the centralized model where there are several issues related to the single point of failure, trust and security, the blockchain utilizes a decentralized approach to use the processing abilities of all the contributing users which deliver better efficiency and eliminate the single point of failure. In addition, blockchain provides better security and data integrity through tamper-proof and immutability features [33].

There are numerous similarities and variances between IoT and blockchain. Table 2 provides a simple comparison between IoT and blockchain.

Table 2. A simple comparison between IoT and blockchain.

Items	IoT	Blockchain
Privacy	Lack of privacy	Ensures the privacy of the participating nodes
Bandwidth	IoT devices have limited bandwidth and resources	High bandwidth consumption
System Structure	Centralized	Decentralized
Scalability	IoT considered to contain a large number of devices	Scales poorly with a large network
Resources	Resource restricted	Resource consuming
Latency	Demands low latency	Block mining is time-consuming
Security	Security is an issue	Has better security

Integrating the blockchain technology with the IoT can resolve several challenges of the centralized IoT model. Table 3 provides a summary of the challenges of the centralized IoT system and how integrating the blockchain with IoT could handle it.

Table 3. Blockchain can provide innovative solutions to issues of the centralized IoT model.

Challenges of Centralized IoT	How Blockchain Can Resolve the Challenge
Security	Blockchain offers better security by utilizing the public key infrastructure that provides more protection against various attacks. In addition, it offers an immutable ledger that cannot be updated only with the approval of the majority of contributing users in the network, which guarantees data integrity. Moreover, all communications between various devices are maintained and secured cryptographically [18].
Scalability	Among the main aspects of the IoT is the enormous number of devices which constantly increases every day. The distributed and decentralized nature of the blockchain can provide an efficient way to provide a scalable way to handle the constant increase in IoT devices.
Point of Failure	The blockchain technology provides distributed and decentralized communication between participating nodes which eliminates the necessity for a central server to manage and control processing and communication operations. Hence, if one device goes down, this will not affect the entire network which overcomes the single point of failure issue associated with the centralized model.
Address Space	The blockchain has a large address space that allows allocating addresses to a large number of devices. The blockchain provides a 160-bit address space which enables the blockchain to assign addresses for a considerable number of objects. Compared to IPv6, blockchain offers 4.3 billion more addresses [34].
Authentication and Access Control	Among the advantages provided by blockchain technology is delivering efficient identity management that helps to build effective authentication and access control. Moreover, smart contracts provide several benefits such as decentralized authentication rules that can be utilized to provide an effective authentication model for various IoT devices.
Data Integrity	Blockchain presents a tamper-proof ability such that a certain transaction cannot be added, edited or deleted only if most of the contributing users in the network verify it. This, in turn, guarantees data integrity.
Susceptibility to Manipulation	The blockchain provides an immutable environment that prevents the manipulation of data to ensure data integrity. In the blockchain, the manipulation or update is only confirmed after the agreement of the majority of participating users.

Table 3. *Cont.*

Challenges of Centralized IoT	How Blockchain Can Resolve the Challenge
Ownership and Identity	Blockchain has the capability to deliver a trustworthy, authorized identity registration, ownership tracking and monitoring. Additionally, it was implemented successfully in various applications especially in the tracking and monitoring goods and products [34].
Flexibility	The blockchain technology provides a flexible environment for various IoT objects through numerous open-source options for blockchain. Moreover, blockchain can scale well to meet the scope and transactional volume of a flexible grid.
Costs and Capacity Constraints	The blockchain provides a decentralized architecture where a central authority or third-party is not required to manage the communications between communicating nodes. This allows for more secure data communication and exchange. In addition, no need for the costs of installing a server with high software and hardware capabilities [7].

4.1. IoT with Blockchain Architecture

Integrating blockchain with IoT has become a necessity to overcome the issues of the centralized IoT architecture and utilize countless benefits of blockchain technology. Implementing the blockchain with IoT can be achieved in numerous ways. This section presents a discussion for one of the approaches of integrating blockchain with the IoT in a layered architecture.

The simple layered blockchain with IoT architecture comprises of four layers. It is the IoT architecture layers discussed in Section 2.2 adding blockchain as a separate layer between network and application layers, as shown in Figure 5.

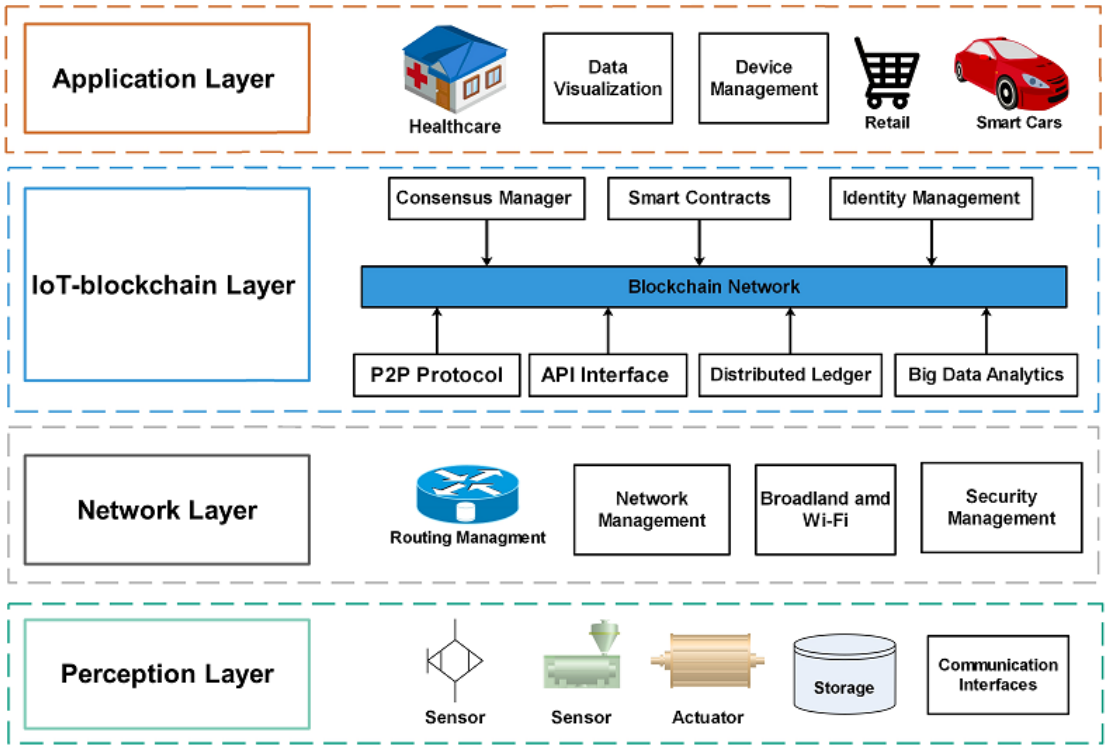

Figure 5. Architecture of IoT with blockchain.

As discussed earlier, the first layer is the perception layer that contains IoT things and objects such as sensors and actuators that are used to sense and perceive the surrounding environment and collect relevant data that can help us understand our surroundings. Then, the network layer that performs network and routing management enables all IoT objects to be linked and communicate together over

the Internet. This layer includes networking and security devices that enable communication and security management.

The newly added layer is named the IoT–blockchain layer, which involves all modules that enable various features of the blockchain technology to be implemented in the IoT system. These features include P2P communication, distributed ledger, smart contracts, Application Programming Interface (API), big data analytics, consensus management, and identity management. P2P protocols are required to enable decentralized communication between various IoT objects. Additionally, the distributed ledger is among the significant features that each IoT device will hold a copy of so that it can be updated with changes in minutes or even seconds within the IoT network [35]. The ledger can be created either with or without permission. The type of ledger will be heavily dependent on the IoT context and the number of nodes in the IoT network.

The big data analytics module enables the blockchain to provide efficient online data storage and processing since the IoT system create huge amounts of data that cannot be processed using traditional methods. In addition, many transactions are deposited in structured ways of ledgers, which will require further data analysis. Smart contracts are also among the important parts of the blockchain technology that used to enable automated decisions based on predetermined conditions. Typically, a smart contract is a software code that runs using blockchain to execute a set of actions when predetermined conditions are met or verified.

Consensus management is also among the main features needed to integrate blockchain with IoT. It acts as the central server that maintains the trust between communicating nodes in the network. Identity management is used to control and identify various nodes in the IoT network. In addition, the API interface enables IoT applications to access blockchain services. The application layer is the top layer that includes various IoT applications and provides data visualization tasks that create numerous digitized services and help decision-makers make accurate and precise decisions based on the collected data from physical IoT devices.

4.2. Implementation of Blockchain with IoT

Blockchain was firstly used for financial transactions and cryptocurrency where transactions are executed and stored by all nodes in the blockchain network. Then, blockchain is integrated in various domains due to the enormous benefits it provides. Among these domains is the IoT system. Combining blockchain with IoT can provide countless benefits for various IoT applications [13]. Meanwhile, the blockchain is decentralized and trustless, as it is suitable for IoT applications such as healthcare, smart homes, smart city, smart transportation and others.

Implementing blockchain in the IoT system is not an easy task. The first and important step is to choose the blockchain platform that will be adopted to merge the IoT with blockchain technology. Ethereum, Hyperledger and IOTA are the most common platforms that can be utilized in implementing blockchain with IoT. Not only are they open-source platforms, but they can also deliver key abilities to connect among blocks, cryptographically secure for the hashing of different transactions minimally in single blocks, advanced marks, consensus, and smart contracts [36].

4.2.1. Ethereum

Ethereum is a multipurpose blockchain platform that was announced in 2013 and then launched in 2015. It produces a universal platform for various blockchain-based applications. It was mainly based on implementing smart contracts, which are programmed codes that are permanently kept on the blockchain and enable executing users' requests. Ethereum also offers a decentralized virtual machine called Ethereum Virtual Machine (EVM) [37].

Although Ethereum is based on smart contracts, the transactions can keep different types of data. This enlarges the likelihood for auditability and allows robust expansion for various IoT applications. Among the drawbacks of Ethereum is that it needs between 10 and 20 s to send a block, which may

create issues in IoT applications that use real-time data. In addition, IoT gadget operations may not promote such a delay [29].

Some studies utilized Ethereum to integrate blockchain with IoT. For instance, Sun et al. [38] proposed Ethereum blockchain-based rich-thin-clients IoT solution to handle issues of resource-constrained IoT when working on the mining of blockchain in IoT applications. Additionally, Mehedi et al. [39] proposed a lightweight masonry for IoT-based blockchains that overcome the memory payload and centralized issues and at the same time improve security and privacy. The authors utilized Ethereum as the blockchain platform to guarantee security, privacy and availability.

4.2.2. Hyperledger

Hyperledger is an open source platform that was designed to help cross-industry blockchain technologies. It is essentially a world-wide open source collaboration involving leaders from numerous industries (about 100 members). Hyperledger is a permissioned blockchain that applies access control, chain code-based smart contracts and variable consensus methods. Although the majority of the distributed records permit open deployment, the permissioned Hyperledger promotes and improves security to avoid various types of attacks, especially Sybil attacks [40]. Since the implementation of smart contracts in Hyperledger is mainly based on chain code implementation, it provides faster execution among peers in several milliseconds. Therefore, adopting chain code smart contracts provides a robust method to implement blockchain in IoT applications [41].

Although there are several frameworks of the Hyperledger, Hyperledger Fabric is among the most common and widely utilized frameworks. It is an open source and modular system. Several studies compare the performance of Ethereum and Hyperledger. For instance, in Franke et al. [42], the authors compared two blockchain platforms to test their feasibility regarding the benefits and restrictions of employing blockchain for the Paris Agreement carbon market mechanism. Furthermore, Pongnumkul et al. [43] performed a performance analysis to assess the performance and limitations of Ethereum and Hyperledger. Their results indicated that Hyperledger Fabric consistently outperformed Ethereum in terms of latency, execution time and throughput.

4.2.3. IOTA

IOTA is not considered as one of the blockchain platforms as it mainly depends on Tangle, another distributed ledger technology. IOTA can be defined as a decentralized platform that facilitates and processes various transactions between communicating devices over the Internet. Basically, IOTA executes a coordinated acyclic chart of transactions instead of chained blocks of numerous transactions. This provides several benefits, for instance, it provides a lightweight solution as consensus does not require the majority of communicating nodes to approve different incremented transactions, instead, two transactions can be verified by single nodes submitting a transaction themselves. This reduces transaction time and overhead [44].

Lightweight and less overhead features of IOTA as well as the use of coordinated acyclic graphs make it among the most adaptable implementations of a distributed record, making it mainly an efficient solution and platform for IoT applications. Many researchers utilized IOTA to provide an efficient platform for IoT applications. For instance, Shabandri and Maheshwari [45] proposed using IOTA to enhance the privacy and security of a smart meter and smart car. The authors presented that IOTA addressed issues related to the limitations of resources in IoT devices and indicated that IOTA eliminated transaction fees and mining which takes large processing power. On the other hand, some researchers indicated that IOTA maybe not the optimal solution for the IoT system. For example, Elsts et al. [46] presented an experimental assessment of IOTA on various IoT platforms. They concluded that the computational overhead of IOTA is high, and it is not an appropriate solution for battery-powered IoT devices. Table 4 provides a comparison between Ethereum, Hyperledger and IOTA.

Table 4. Comparison between Ethereum, Hyperledger and IOTA.

Item	Ethereum	Hyperledger	IOTA
Transaction Time	10–15 s	0.05–100 ms	120 s
Consensus Mechanism	Proof of Work (PoW)	Practical byzantine fault tolerance (PBFT)	N/A
Network Usage	Less usage	High usage	Less usage
Computation Cost	High computation cost	Less computation cost	Less computation cost
Smart Contracts	Yes	Yes	No

4.3. Recent Studies of IoT with Blockchain

Integrating blockchain technology with IoT is among the most modern subjects that has attracted the courtesy of various researchers to overcome issues of centralized IoT architecture. For example, several studies presented the blockchain as the ultimate solution to tackle security and privacy challenges in the IoT system. For instance, Khan and Salah [22] presented a review of IoT and its security challenges concerning IoT-layered architectures. Then, the authors identified security requirements of the IoT system and state-of-the-art solutions. The paper also presented blockchain technology as a vital empowering to resolve most of the security issues of the IoT system. Moreover, Sengupta et al. [47] provided a review of security attacks and issues in the IoT and industrial IoT (IIoT) and classify it based on the vulnerability. Then, the authors presented the blockchain technology and how it can resolve some of the aforementioned security issues. Besides, they presented some of the challenges of blockchain with IIoT.

In the same way, Banejee et al. [48] provided a review of IoT security solutions and discussed issues of lack of IoT datasets for researchers and practitioners. Then, the authors proposed the blockchain to provide a secure environment for sharing IoT datasets. They also discussed some of the challenges of blockchain technology. In addition, Dorri et al. [49] proposed a lightweight architecture for IoT based on blockchain technology to provide a secure and private IoT system and at the same time eliminate the overhead of blockchain. Moreover, Polyzos and Fotiou [50] review the potential of blockchain technology to investigate the security requirements of the IoT system and how integrating the IoT with blockchain can solve these security challenges.

Moreover, Karthikeyan et al. [51] provided a review of IoT security issues, then proposed the blockchain as a suggested solution to resolve these issues. They also discussed the potentials of integrating IoT with blockchain. In addition, Fotiou et al. [52] suggested a smart contract-based solution to handle security and privacy issues in the IoT system and to make the IoT device communicate securely. Their proposed solution enabled decentralization for access control, authentication and payments depending on blockchain technology.

Tandon [53] provided a review of blockchain technology and how it provides the ultimate solution to handle the security and privacy challenges associated with the IoT system. The paper also discussed the benefits and challenges of integrating blockchain with IoT. In the same way, Zhu and Badr [54] provided a review to define the demands of creating an identity management system for IoT. Then, they proposed that blockchain technology be integrated with the IoT to build an efficient identity management system to provide better trust and performance. Moreover, Hang and Kim [35] proposed an integrated IoT platform using blockchain technology to ensure sensing data integrity. Their platform enabled real-time monitoring and control between the end-user and device. The results demonstrated that their platform could be a good solution for resource-constrained IoT devices. Additionally, Kadam and John [55] proposed a framework based on the Ethereum blockchain for low-power IoT devices to solve the power issue in IoT devices while communicating, validating transactions and providing security.

Blockchain technology was presented as a solution to provide an efficient and effective access control system. For example, Dukkipati et al. [56] proposed a blockchain-based access control model to

handle security and privacy challenges in the IoT system. They employed blockchain as decentralized access manager which provides the access decision. Moreover, Novo [57] suggested a blockchain-based distributed control model for the IoT system. The author claimed that the blockchain could provide efficient access control management in the IoT applications. Besides, Zhang et al. [58] have suggested a smart contract-based access control framework that contained several access control contracts (ACCs). They utilized smart contracts to achieve a trusted and distributed access control model for the IoT.

Blockchain was also proposed as an efficient solution to enhance the security and privacy of healthcare data. For example, Badr et al. [59] utilized the blockchain to enhance the privacy of patient data. They suggested a protocol for protecting the privacy of eHealth data (EHRs) based on pseudonym-based encryption with different authorities (PBE-DA). Furthermore, they utilized blockchain as a stage between IoT medical devices and the healthcare system. Additionally, Mishra and Tyagi [60] proposed an intrusion detection system for the IoT based on blockchain technology to detect unauthorized access and filter network traffic. They applied their proposal to the healthcare domain to protect patient information.

Another domain in which blockchain technology was deployed was agriculture. Several researchers proposed utilizing blockchain to overcome the issues of existing systems. For instance, Patil et al. [61] suggested a lightweight architecture for smart greenhouse farms based on blockchain to improve security and privacy in agriculture. The blockchain makes IoT devices in greenhouses act as immutable ledgers. Moreover, Lin et al. [62] suggested an open, self-organized and trusted food traceability system by integrating blockchain with IoT. Their proposed system replaced labour-intensive recording and minimized human involvement, which created a smart agriculture system. Besides, Dogo et al. [63] proposed a framework for utilizing blockchain in agriculture. They showed technological benefits and technical advantages of integrating blockchain and IoT in agriculture to improve security, transparency and overall efficiency. In addition, Kamilaris et al. [64] provided a discussion of the use of the blockchain in agriculture and food chain by investigating benefits and challenges.

Blockchain was adopted in the supply chain as well. Rejeb et al. [65] provided a review of the deployment of blockchain technology with IoT and potential benefits of this integration on the supply chain domain. They also discussed the impact of blockchain on key features of the IoT system. Moreover, Huckle et al. [66] provided a discussion of the use of the blockchain with IoT to deliver its safe and distributed application in the economy. Additionally, blockchain was adopted in E-business and payments, for example, Zhang and Wen [67] suggested an IoT E-business system based on blockchain technology. They utilized decentralization and smart contracts to achieve integration with the IoT system. Moreover, Ruta et al. [68] suggested a blockchain-based service-oriented model. They utilized smart contracts to enable distributed and decentralized execution and trust. Besides, Huh et al. [69] proposed using Ethereum smart contract to store the data produced by IoT devices like smart meters and phones. They utilized Ethereum smart contracts to control the usage of electricity through the smartphone.

Reviewing the benefits, constraints and issues of integrating blockchain with IoT was among the topics that attracted many researchers. Some researchers provided a systematic literature review to help the reader obtain a precise knowledge about certain research questions. For example, Conoscenti et al. [70] provided a systematic literature review to collect information and knowledge on the present uses of blockchain technology to validate its ability to provide better security, anonymity and adaptability over existing technologies. They also categorised the current uses of the blockchain. Moreover, Lo et al. [71] provided a systematic literature review to analyse various solutions suggested by different researchers to converge the blockchain with the IoT. They reviewed publications that involved the implementation of blockchain with IoT. In the same way, Abadi et al. [72] provided a systematic literature review of integrating blockchain with IoT.

Other researchers provided reviews and surveys to investigate the integration of blockchain with IoT. Wang et al. [73] provided a survey of blockchain technologies and their effect on IoT applications.

They also explained the effect of consensus protocols and data structure of the blockchain on improving the IoT system by discussing some of the open issues of blockchain. In addition, Thakore et al. [74] examined the integration of IoT with blockchain and how to create a mixture that provides a better outcome. They presented the basic fundamentals of both technologies by explaining their protocols and functioning. Besides, Ferrag et al. [75] provided a review paper that investigated the role of blockchain in various applications of IoT like healthcare or smart vehicles. They also discussed the benefits of blockchain regarding security, performance and complexity.

In the same way, Dai et al. [76] presented a review of blockchain with IoT and the challenges resulting from this integration in the context of IIoT and 5G. Moreover, Atlam and Wills [5] discussed the integration of distributed ledger technology with the IoT system. They investigated types of distributed ledger technologies and focused on the blockchain and its main potentials and challenges with the IoT system. Besides, Maroufi et al. [77], Alamri et al. [78], and Atlam et al. [18] presented a review of the integration of IoT with blockchain by investigating the advantages and shortcomings. Moreover, Lao et al. [79] provided a survey of the key elements that were needed to integrate blockchain with IoT. They focused on various consensus mechanisms that could be utilized in IoT with blockchain. Table 5 summarizes the contribution of recent studies that examined the integration of blockchain with IoT.

Table 5. Summarized contributions of recent studies that examined the integration of blockchain with IoT.

Citation	Summary of Contribution
Khan and Salah [22]	A review of IoT security challenges and how blockchain can handle most IoT security challenges.
Wang et al. [73]	A survey of blockchain technologies and their effect on IoT applications.
Badr et al. [59]	Proposed protocol for preserving the privacy of EHRs based on pseudonym-based encryption with different authorities (PBE-DA).
Kamilaris et al. [64]	An examination of the use of blockchain technology in agriculture by highlighting benefits and challenges.
Sengupta et al. [47]	A review of security issues in the IIoT. Authors also discussed how blockchain can resolve these issues in the IIoT context.
Huckle et al. [66]	A discussion of the use of the blockchain with IoT to deliver a secure economy.
Thakore et al. [74]	Basic review of fundamentals of IoT and blockchain and how to create a mixture that provides a better outcome.
Banejee et al. [48]	A review of IoT security solutions and challenges of the lack of IoT datasets. Then, proposed utilizing blockchain to share IoT datasets securely.
Lin et al. [62]	Suggested an open, self-organized and trusted food traceability by integrating blockchain with IoT.
Patil et al. [61]	Proposed a lightweight architecture for smart greenhouse farms based on blockchain to improve security and privacy.
Dogo et al. [63]	Suggested a framework for applying blockchain in agriculture to improve security, transparency and efficiency.
Ferrag et al. [75]	A survey to investigate the role of blockchain in various applications of IoT like healthcare and smart vehicles.
Kadam and John [55]	Proposed a framework based on Ethereum blockchain for low-power IoT devices to solve the power issue in IoT devices.
Dorri et al. [49]	Suggested a blockchain-based lightweight architecture for IoT to deliver a protected and private IoT system.
Maroufi et al. [77]	Provided a review of the convergence of IoT with blockchain by investigating benefits and shortcomings.
Dai et al. [76]	Introduced a review of blockchain with IoT and challenges results from this integration in the context of IIoT and 5G.

Table 5. *Cont.*

Citation	Summary of Contribution
Alamri et al. [78]	Provided a review of the convergence of IoT with blockchain by investigating advantages and shortcomings.
Dukkipati et al. [56]	Suggested a blockchain-based access control model to resolve IoT security and privacy challenges.
Lao et al. [79]	Presented a review of the key elements that needed to integrate blockchain with IoT.
Conoscenti et al. [70]	Provided a systematic literature review to collect information and knowledge on the present uses of the blockchain.
Polyzos and Fotiou [50]	Provided a review of the potentials of blockchain to solve IoT security.
Atlam and Wills [5]	Presented a review of the convergence of distributed ledger technology with the IoT system. They also investigated the blockchain and its main potential and challenges with the IoT system.
Novo [57]	Proposed a blockchain-based distributed access control system for the IoT system.
Lo et al. [71]	Presented a systematic literature review to analyse various solutions suggested by different researchers to converge the blockchain with the IoT.
Abadi et al. [72]	Provided a systematic literature review of integrating the blockchain with IoT.
Karthikeyan et al. [51]	Presented a review of IoT security issues, then proposed the blockchain as a suggested solution to resolve these issues.
Mishra and Tyagi [60]	Proposed a blockchain-based intrusion detection system for the IoT to detect unauthorized access and filter network traffic.
Fotiou et al. [52]	Suggested a smart contract-based solution to resolve security and privacy challenges in the IoT system and make the IoT device communicate securely.
Rejeb et al. [65]	Provided a survey of the deployment of Blockchain technology with IoT and the potential benefits of this integration on the supply chain domain.
Tandon [53]	Provided a review of blockchain technology and how it provides the ultimate solution to resolve security and privacy challenges associated with the IoT system.
Atlam et al. [18]	Presented a discussion of the convergence of the IoT with blockchain by explaining the benefits, opportunities and challenges of this integration.
Hang and Kim [35]	Proposed an integrated IoT platform using the blockchain to ensure the data integrity of the data collected from sensors.
Zhang and Wen [67]	Suggested an IoT E-business model based on blockchain technology using features of decentralization and smart contracts to produce an efficient business model.
Zhu and Badr [54]	Provided a review to define the demands of creating an identity management system for IoT. Then, the paper proposed blockchain to be integrated with the IoT to build an efficient identity management system.
Ruta et al. [68]	Proposed a blockchain-based service-oriented model for registration, discovery, selection and payment.
Zhang et al. [58]	Suggested a smart contract-based access control model to achieve a trusted and distributed access model for the IoT system.
Huh et al. [69]	Proposed using Ethereum smart contract to store the data produced by IoT devices such as smart meters and phones.

Moreover, Table 6 categorises recent studies which investigated the integration of blockchain with IoT which can help researchers to track recent studies and publications that adopted blockchain with IoT in a certain domain.

Table 6. Categorisation of the recent studies of blockchain (BC) with IoT.

Citation	Survey	Systematic Review	BC for IoT Security	BC for IoT Privacy	BC for Supply Chain	BC for Healthcare	BC for Agriculture
Khan and Salah [22]	√	-	√	-	-	-	-
Wang et al. [73]	√	-	-	-	-	-	-
Badr et al. [59]	-	-	-	√	-	√	-
Kamilaris et al. [64]	-	-	-	-	-	-	√
Sengupta et al. [47]	√	-	√	-	-	-	-
Huckle et al. [66]	√	-	-	-	√	-	-
Thakore et al. [74]	√	-	-	-	-	-	-
Banejee et al. [48]	√	-	√	-	-	-	-
Lin et al. [62]	-	-	-	-	-	-	√
Patil et al. [61]	-	-	-	-	-	-	√
Dogo et al. [63]	-	-	-	-	-	-	√
Ferrag et al. [75]	√	-	-	-	-	-	-
Kadam and John [55]	-	-	√	√	-	-	-
Dorri et al. [49]	-	-	√	-	-	-	-
Maroufi et al. [77]	√	-	-	-	-	-	-
Dai et al. [76]	√	-	-	-	√	-	-
Alamri et al. [78]	√	-	-	-	-	-	-
Dukkipati et al. [56]	-	-	√	√	-	-	-
Lao et al. [79]	√	-	-	-	-	-	-
Conoscenti et al. [70]	√	-	-	-	-	-	-
Polyzos and Fotiou [50]	√	-	√	-	-	-	-
Atlam and Wills [5]	√	-	√	√	-	-	-
Novo [57]	-	-	√	-	-	-	-
Lo et al. [71]	-	√	-	-	-	-	-
Abadi et al. [72]	-	√	-	-	-	-	-
Karthikeyan et al. [51]	√	-	√	-	-	-	-
Mishra and Tyagi [60]	-	-	√	-	-	√	-
Fotiou et al. [52]	-	-	√	√	-	-	-
Rejeb et al. [65]	√	-		-	√	-	-
Tandon [53]	√	-	√	-	-	-	-
Atlam et al. [18]	√	-		-	-	-	-
Hang and Kim [35]	-	-	√	-	-	-	-
Zhang and Wen [67]	-	√	-	-	-	√	-
Zhu and Badr [54]	√	-	√	√	-	-	-
Ruta et al. [68]	√	-	-	-	√	-	-
Zhang et al. [58]	-	-	√	-	-	-	-
Huh et al. [69]	√	-	√	-	-	-	-

5. Blockchain as a Service for IoT

Blockchain, as a technology, has the ability to provide a service layer that makes it easier to be integrated with the IoT architecture as described earlier in Figure 5. Blockchain technology and its features can be implemented to the whole digital realm, not just in cryptocurrency, to strengthen hundreds of industries by eliminating intermediaries and reduce costs. As cloud computing can provide different services to their users such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), blockchain can be used as a service that can be used by different IoT applications. This creates what is called Blockchain as a Service (BaaS).

Typically, BaaS refers to creating, controlling, hosting and utilizing numerous features of blockchain technology such as smart contracts, immutability, tamper-proof, and distributed ledger, on cloud computing. Hence, blockchain can provide different services based on the cloud computing

infrastructure. These services will be required for Fog nodes (IoT devices) to benefit and utilize the advantages of blockchain technology in the IoT context. BaaS can be implemented for IoT devices explicitly as PaaS or implicitly as SaaS. While implementing blockchain on-premise is very costly, as it needs high-cost equipment to build the infrastructure and performance of the distributed ledger technology [80]. BaaS is currently being presented by platforms such as Amazon, Microsoft Azure, Oracle, IBM Blockchain. The architecture of BaaS is shown in Figure 6.

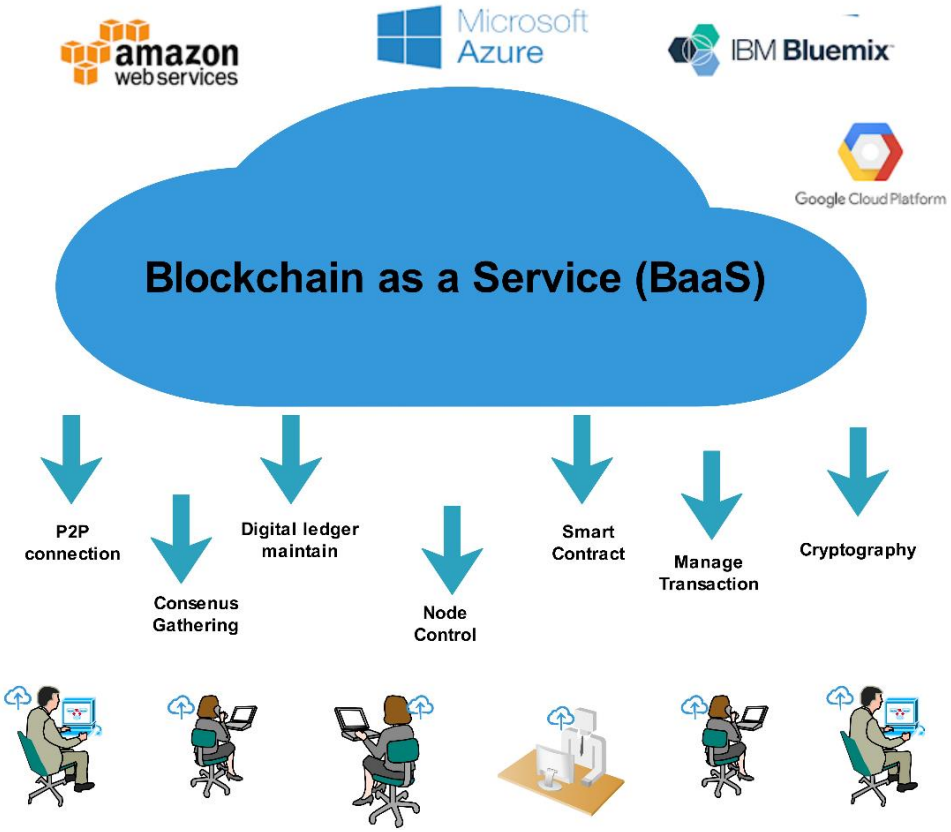

Figure 6. Typical Architecture of BaaS.

BaaS can be used to provide several advantages for various IoT applications. For instance, with the pre-built cloud platforms, BaaS can be utilized more easily and cheaply than on-premise implementation. Moreover, since BaaS exists with other cloud services (SaaS, PaaS, IaaS), this will allow blockchain to be deployed with various cloud and IoT applications and increase the interoperability of blockchain technology with these different applications. In addition, among the other benefits BaaS can provide is usability. In other words, implementing a blockchain using one of blockchain platforms needs a good level of skills in cryptography and distributed technologies. Alternatively, BaaS can be delivered as a full service by the service provider, which allows the user to deploy, control and run blockchain technology without the need for any technical skills.

6. AI with Blockchain and IoT

There is no doubt that AI has become one of the topics that has significant effects on different domains. According to the Merriam-Webster dictionary, AI is defined as "the capability of a machine to imitate intelligent human behaviour" [81]. The key issue of AI is to produce new models and approaches that can provide smart activities. Typically, AI is mainly based on experiments in which the researcher uses the computer system as a lab to execute the validation and testing of their hypotheses [82].

Integrating the IoT with AI has the ability to produce a robust technology that is able to resolve several IoT issues that are associated with the vast volume of data produced by billions of IoT devices.

Analysing these vast amounts of data with traditional analytics methods will not be viable, instead, adopting various AI and machine learning methods will have the ability to analyse and extract meaningful information to profit from the full benefits of IoT data [83]. With the massive analytic abilities of AI, numerous governments and organizations have started adopting AI methods as a way to unlock the value of vast amounts of IoT data. Although the invention of fog/edge computing minimized the response time that allows real-time-based IoT applications to grow significantly, adopting AI approaches will have the capability to provide better performance in a very short response time. In addition, the integration of AI with IoT can improve security, not only by combat external threat but also provide an effective way to predict those threats.

On the other hand, integrating AI with blockchain can have a good effect on both technologies. For AI, blockchain can resolve several issues of AI, for example, transparency. AI is a block-box for users that lack explainability. With the transparency of blockchain by sharing the ledger to all its nodes and audit trail that provides a clear method for tracking data back to the machine decision process, this will optimize the trustworthiness of data and AI. In addition, blockchain can improve AI effectiveness to secure data sharing that allows having more data, which in turn increases training data and produces better AI models. Moreover, implementing AI with smart contracts can decrease risk scenarios, as smart contracts are programmed to perform specific actions when the conditions are met [5].

For blockchain, AI can resolve some of the limitations of blockchain technology, for instance, consensus mechanisms. Utilizing AI in PoW or PoS can allow nodes to validate the transactions quickly and efficiently. Furthermore, AI can improve energy consumption in blockchain since the mining process needs huge amounts of energy by adopting AI approaches which have demonstrated effectiveness in improving energy consumption [84]. Moreover, adopting AI can resolve the scalability issues of blockchain by adopting federated learning, as an example, that is able to provide a decentralized learning system. In addition, although blockchain provides better security over existing technologies, AI can provide an additional layer of security [84,85].

Although the combination of the three technologies of Blockchain, AI and IoT is still in the development stage, there are numerous expectations that it could have a significant effect on both the global economy and the way we live. Integrating these technologies will provide a new perspective on our future and world. It will create a world where the data of our environment/world are collected through IoT devices, and analysis and decisions are on our behalf by AI, before being stored and time-stamped on blockchain as a permanent record that is communicated and shared on our behalf [85]. Therefore, there is a need for research to investigate the possible and best ways of integrating these technologies to experience from their full benefits.

7. Future Research Directions of IoT with Blockchain

Despite the integration of IoT with blockchain has several advantages, it also brings multiple issues that need to be resolved to obtain the full benefits of both technologies. This section provides a discussion of future research directions of IoT with blockchain technology.

7.1. Security

The IoT system involves billions of heterogeneous IoT objects that are designed with little security in the consideration of their manufactures. These devices with poor built-in security procedures are a simple mark for various security attackers. Although incorporating IoT with blockchain technology can improve the IoT security by utilizing encryption, immutability, tamper-proof and digital signature features of blockchain technology, the security is still one of the challenges in implementing an efficient and effective IoT system with blockchain [86].

With the increasing adoption of IoT devices and applications, there is an increasing direction towards expanding the use of wireless networks, especially in industrial domains. Although wireless communication provides several advantages, it also suffers from several security vulnerabilities like

replaying attacks, passive eavesdropping, and jamming [51]. Besides, due to the limitations of resources in IoT devices, sophisticated and advanced encryption algorithms cannot be utilized in the IoT system. Meanwhile, blockchain technology has its security weaknesses. For example, there are program defects of smart contracts and decentralized autonomous organization (DAO) attack [73]. Therefore, there is a need for more research to investigate security issues in IoT and blockchain.

7.2. Scalability

Among the key issues of integrating blockchain with IoT is the ability of the blockchain to scale and work efficiently with a large-scale network like the IoT. The throughput of transactions per second can be used to measure the scalability of blockchain against the number of IoT devices. Blockchain platforms provide poor throughput. For example, Bitcoin can only process seven transactions per second. Moreover, Ethereum can only process 20 transactions per second. In contrast, VISA can process nearly 2000 transactions per second and PayPal has a throughput of 170 transactions per second [87].

Therefore, this processing speed cannot address the demands of the IoT which contains billions of transactions. Moreover, several IoT applications are mainly working with real-time data, with limited throughput of blockchain, so these applications will face complications in order work efficiently. Although there are several suggested solutions to resolve the scalability issue of blockchain technology such as building more scalable consensus algorithms and designing private blockchain for IoT, there is a need for more research to discover an efficient solution to this issue [88].

7.3. Data Storage

Blockchain is not built to record vast volumes of data. In contrast, the IoT system is considered as one of the sources of big data. The storage capacity is among the major issues of blockchain technology. The size of the entire Bitcoin blockchain is around 150 gigabytes, also, the size of the entire Ethereum Blockchain is around 400 gigabytes. Storing all blocks of the blockchain is required. Without having all previous blocks, IoT devices cannot validate the transactions produced by other devices. Besides, historical data are required to produce new transactions [89]. Hence, all data created by IoT devices, which are in Zettabytes, need to be stored on the blockchain, which is not feasible.

In addition, the cost of storing data on the blockchain is very expensive. For instance, the cost of storing one Gigabyte of data is about USD 200,000 in Ethereum [73]. This price is not practical for various IoT applications and services. Indeed, the convergence of IoT with blockchain removes the necessity for a centralized server to keep IoT data, however, data storage in the blockchain is very difficult and expensive. Hence, there is a need for more research to investigate new methods to resolve this issue.

7.4. Legal Issues

Any new technology such as IoT and blockchain is affected by regulation and laws of each nation. Among the issues that stand in the way of integrating IoT and blockchain successfully is the lack of laws, especially regarding blockchain. Since blockchain provides anonymity features, it is very difficult to identify the real identities of their users, making it a suitable environment for criminals. Therefore, different countries still have several issues about how to deal with blockchain technology and what are suitable laws and regulations that can be used to control such a new environment [32].

In the same way, IoT devices collect a huge amount of data about their owners. This information can include sensitive and confidential data. Most IoT devices share this information with their manufactures or service providers without having authorization from their owners. This completely violates the privacy of the devices' owners [90].

7.5. Limited Resources

Most IoT devices have limited resources in terms of memory, processing power and energy. For instance, smart meters have low battery power, limited storage and low computing. Integrating

such resource-constrained IoT devices with blockchain technology will face several issues. For instance, consensus mechanisms need exhaustive processing power and consume intensive energy. Hence, consensus mechanisms with enormous processing and power demands cannot operate with IoT devices with limited resources. Moreover, as discussed earlier, the storage capacity is among the major issues of blockchain, as the total size of Bitcoin and Ethereum blockchains are around 150 and 400 gigabytes respectively. However, IoT devices generate data in Zettabytes. Therefore, blockchain is not suitable for storing IoT data [3,91].

Possible solutions to this issue may be integrating cloud computing with IoT and blockchain to resolve issues of the resource constraints of IoT objects [92]. The main issue will be how to integrate centralized cloud computing with blockchain to provide efficient resultant technology.

8. Conclusions

With several challenges presented in the centralized IoT architecture, moving the IoT into one of the distributed ledger technologies may be the correct choice. Among the common types of distributed ledger technologies is the blockchain. It utilizes a decentralized approach which delivers better efficiency and eliminates the single point of failure. Moreover, blockchain delivers better security and data integrity through tamper-proof and immutability features. The integration of blockchain with IoT can resolve issues of the IoT centralized system and provides a good way for future developments. Therefore, the objective of this paper was to provide a comprehensive discussion of integrating the IoT system with blockchain technology. After presenting the basis of IoT and blockchain, the paper presented a comprehensive discussion of integrating IoT with blockchain by highlighting how blockchain resolved issues of IoT. Besides, recent studies presenting the convergence of IoT with blockchain are also presented. Then, blockchain as a service for the IoT is discussed to show how various features of blockchain technology can be implemented as a service for various IoT applications. This was followed by discussing the impact of integrating AI on both IoT and blockchain. To this end, future research directions of IoT with blockchain were discussed.

Author Contributions: H.F.A. designed and developed the structure and writing of the manuscript. M.A.A. and A.G.A. have been involved in drafting the manuscript, while G.W. contributed to the abstract part and reviewed the completed manuscript before submission. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Atlam, H.F.; Walters, R.J.; Wills, G.B. Internet of Things: State-of-the-art, Challenges, Applications, and Open Issues. *Int. J. Intell. Comput. Res.* **2018**, *9*, 928–938. [CrossRef]
2. Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Alshdadi, A.A.; Wills, G.B. Security, Cybercrime and Digital Forensics for IoT. In *Greedoids*; Springer Science and Business Media LLC: Berlin, Germany, 2019; Volume 174, pp. 551–577.
3. Atlam, H.F.; Alenezi, A.; Alassafi, M.O.; Wills, G.B. Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. *Int. J. Intell. Syst. Appl.* **2018**, *10*, 40–48. [CrossRef]
4. Fernandez-Carames, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* **2018**, *6*, 32979–33001. [CrossRef]
5. Atlam, H.F.; Wills, G.B. Intersections between IoT and distributed ledger. In *Advances in Organometallic Chemistry Volume 60*; Elsevier BV: Amsterdam, The Netherlands, 2019; pp. 73–113.
6. Karafiloski, E.; Mishev, A. Blockchain solutions for big data challenges: A literature review. In Proceedings of the IEEE EUROCON 2017—17th International Conference on Smart Technologies, Ohrid, Macedonia, 6–8 July 2017; pp. 763–768. [CrossRef]
7. 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]

8. ITU. Overview of the Internet of Things. Available online: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=y.2060 (accessed on 13 October 2020).
9. Statista. Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025 (in Billions). 2018. Available online: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (accessed on 8 October 2020).
10. Atlam, H.F.; Wills, G.B. Technical aspects of blockchain and IoT. In *Advances in Organometallic Chemistry Volume 60*; Elsevier BV: Amsterdam, The Netherlands, 2019; pp. 1–39.
11. Hugoson, M.Å. Centralized versus Decentralized Information Systems: A Historical Flashback. *IFIP Adv. Inf. Commun. Technol.* **2008**, *303*, 106–115.
12. Yin, S.; Lu, Y.; Li, Y. Design and implementation of IoT centralized management model with linkage policy. In Proceedings of the Third International Conference on Cyberspace Technology (CCT 2015), Beijing, China, 17–18 October 2015; pp. 5–9. [CrossRef]
13. Atlam, H.F.; Wills, G.B. IoT Security, Privacy, Safety and Ethics. In *Intelligent Sensing, Instrumentation and Measurements*; Springer Science and Business Media LLC: Berlin, Germany, 2019; pp. 123–149.
14. Atlam, H.F.; Walters, R.J.; Wills, G.B. Internet of Nano Things. In Proceedings of the 2nd International Conference on Cloud and Big Data Computing (ICCBDC 2018), Barcelona, Spain, 3–5 August 2018; pp. 71–77. [CrossRef]
15. Atlam, H.F.; Walters, R.J.; Wills, G.B. Intelligence of Things: Opportunities & Challenges. In Proceedings of the 2018 3rd Cloudification of the Internet of Things (CIoT), Paris, France, 2–4 July 2018; pp. 1–6.
16. Conoscenti, M.; Vetro, A.; De Martin, J.C. Peer to Peer for Privacy and Decentralization in the Internet of Things. In Proceedings of the 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), Buenos Aires, Argentina, 20–28 May 2017; pp. 288–290.
17. Atlam, H.F.; Walters, R.J.; Wills, G.B. Fog Computing and the Internet of Things: A Review. *Big Data Cogn. Comput.* **2018**, *2*, 10. [CrossRef]
18. Atlam, H.F.; Wills, G.B. An efficient security risk estimation technique for Risk-based access control model for IoT. *Internet Things* **2019**, *6*, 1–20. [CrossRef]
19. Atlam, H.F.; Alenezi, A.; Walters, R.J.; Wills, G.B.; Daniel, J. Developing an Adaptive Risk-Based Access Control Model for the Internet of Things. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 655–661. [CrossRef]
20. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Available online: https://git.dhimmel.com/bitcoin-whitepaper/ (accessed on 13 October 2020).
21. Back, A.; Corallo, M.; Dashjr, L.; Friedenbach, M.; Maxwell, G.; Miller, A.; Poelstra, A.; Timón, J.; Wuille, P. Enabling Blockchain Innovations with Pegged Sidechains. 2014. Available online: http://kevinriggen.com/files/sidechains.pdf (accessed on 13 October 2020).
22. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
23. Coinbase. What Is the Bitcoin Blockchain? 2017. Available online: https://support.coinbase.com/customer/portal/articles/1819222-what-is-the-blockchain (accessed on 8 October 2020).
24. Oxford. Blockchain|Definition of Blockchain in English by Oxford Dictionaries. 2018. Available online: https://en.oxforddictionaries.com/definition/blockchain (accessed on 8 October 2020).
25. Sultan, K.; Ruhi, U.; Lakhani, R. Conceptualizing Blockchains: Characteristics & Applications. *arXiv* **2018**, arXiv:1806.03693.
26. Sikorski, J.J.; Haughton, J.; Kraft, M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Appl. Energy* **2017**, *195*, 234–246. [CrossRef]
27. Biswas, K.; Muthukkumarasamy, V. Securing Smart Cities Using Blockchain Technology. In Proceedings of the 2016 IEEE 18th International Conference on High Performance Computing and Communications and IEEE 14th International Conference on Smart City and IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, Australia, 12–14 December 2016; pp. 5–6.
28. Wu, H.; Li, Z.; King, B.; Ben Miled, Z.; Wassick, J.; Tazelaar, J. A Distributed Ledger for Supply Chain Physical Distribution Visibility. *Information* **2017**, *8*, 137. [CrossRef]

29. Atlam, H.F.; Azad, M.A.; Alassafi, M.O.; Alshdadi, A.A.; Alenezi, A. Risk-Based Access Control Model: A Systematic Literature Review. *Future Internet* **2020**, *12*, 103. [CrossRef]
30. Heilman, E.; Baldimtsi, F.; Goldberg, S. Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions. In Proceedings of the Computer Vision; Springer Science and Business Media LLC: Berlin, Germany, 2016; Volume 9604, pp. 43–60.
31. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
32. Fabiano, N. Internet of Things and Blockchain: Legal Issues and Privacy. The Challenge for a Privacy Standard. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 727–734.
33. Ferraro, P.; King, C.; Shorten, R. Distributed Ledger Technology for Smart Cities, the Sharing Economy, and Social Compliance. *IEEE Access* **2018**, *6*, 62728–62746. [CrossRef]
34. Alkurdi, F.; Elgendi, I.; Munasinghe, K.S.; Sharma, D.; Jamalipour, A. Blockchain in IoT Security: A Survey. In Proceedings of the 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, Australia, 21–23 November 2018; pp. 1–4. [CrossRef]
35. Hang, L.; Kim, D.-H. Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. *Sensors* **2019**, *19*, 2228. [CrossRef]
36. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT Integration: A Systematic Survey. *Sensors* **2018**, *18*, 2575. [CrossRef]
37. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
38. Sun, H.; Hua, S.; Zhou, E.; Pi, B.; Sun, J.; Yamashita, K. Using Ethereum Blockchain in Internet of Things: A Solution for Electric Vehicle Battery Refueling. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2018; Volume 10974, pp. 3–17.
39. Mehedi, S.K.T.; Shamim, A.A.M.; Miah, M.B.A. Blockchain-based security management of IoT infrastructure with Ethereum transactions. *Iran J. Comput. Sci.* **2019**, *2*, 189–195. [CrossRef]
40. Samaniego, M.; Deters, R. Hosting Virtual IoT Resources on Edge-Hosts with Blockchain. In Proceedings of the 2016 IEEE International Conference on Computer and Information Technology (CIT), Nadi, Fiji, 8–10 December 2016; pp. 116–119.
41. Cachin, C. Architecture of the Hyperledger Blockchain Fabric. In Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers, Chicago, Illinois, 25–29 July 2016.
42. Franke, L.A.; Schletz, M.; Salomo, S. Designing a Blockchain Model for the Paris Agreement's Carbon Market Mechanism. *Sustainability* **2020**, *12*, 1068. [CrossRef]
43. Pongnumkul, S.; Siripanpornchana, C.; Thajchayapong, S. Performance Analysis of Private Blockchain Platforms in Varying Workloads. In Proceedings of the 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 31 July–3 August 2017; pp. 1–6.
44. Raschendorfer, A.; Mörzinger, B.; Steinberger, E.; Pelzmann, P.; Oswald, R.; Stadler, M.; Bleicher, F. On IOTA as a potential enabler for an M2M economy in manufacturing. *Procedia CIRP* **2019**, *79*, 379–384. [CrossRef]
45. Shabandri, B.; Maheshwari, P. Enhancing IoT Security and Privacy Using Distributed Ledgers with IOTA and the Tangle. In Proceedings of the 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 7–8 March 2019; pp. 1069–1075.
46. Elsts, A.; Mitskas, E.; Oikonomou, G. Distributed Ledger Technology and the Internet of Things. In Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems—BlockSys'18, Shenzhen, China, 4 November 2018; pp. 7–12.
47. Sengupta, J.; Ruj, S.; Das Bit, S. A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT. *J. Netw. Comput. Appl.* **2020**, *149*, 102481. [CrossRef]
48. Banerjee, M.; Lee, J.; Choo, K.-K.R. A blockchain future for internet of things security: A position paper. *Digit. Commun. Netw.* **2018**, *4*, 149–160. [CrossRef]
49. Dorri, A.; Kanhere, S.S.; Jurdak, R. Blockchain in internet of things: Challenges and Solutions. *arXiv* **2016**, arXiv:1608.05187.

50. Polyzos, G.C.; Fotiou, N. Blockchain-Assisted Information Distribution for the Internet of Things. In Proceedings of the 2017 IEEE International Conference on Information Reuse and Integration (IRI), San Diego, CA, USA, 4–6 August 2017; pp. 75–78.
51. Karthikeyyan, P.; Velliangiri, S.; S, I.T.J. Review of Blockchain based IoT application and its security issues. In Proceedings of the 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, India, 5–6 July 2019; pp. 6–11. [CrossRef]
52. Fotiou, N.; Siris, V.A.; Polyzos, G.C. Interacting with the Internet of Things Using Smart Contracts and Blockchain Technologies. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2018; Volume 11342, pp. 443–452.
53. Tandon, A. An empirical analysis of using blockchain technology with internet of things and its application. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 1470–1475.
54. Zhu, X.; Badr, Y. Identity Management Systems for the Internet of Things: A Survey towards Blockchain Solutions. *Sensors* **2018**, *18*, 4215. [CrossRef]
55. Kadam, S.B.; John, S.K. *Blockchain Integration with Low-Power Internet of Things Devices*; Elsevier BV: Amsterdam, The Netherlands, 2020; pp. 183–211.
56. Dukkipati, C.; Zhang, Y.; Cheng, L.C. Decentralized, BlockChain Based Access Control Framework for the Heterogeneous Internet of Things. In Proceedings of the Third ACM Workshop on Attribute-Based Access Control—ABAC'18, Tempe, AZ, USA, 19–21 March 2018; pp. 61–69.
57. Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. *IEEE Int. Things J.* **2018**, *5*, 1184–1195. [CrossRef]
58. Zhang, Y.; Kasahara, S.; Shen, Y.; Jiang, X.; Wan, J. Smart Contract-Based Access Control for the Internet of Things. *IEEE Int. Things J.* **2018**, *6*, 1594–1605. [CrossRef]
59. Badr, S.; Gomaa, I.; Abd-Elrahman, E. Multi-tier Blockchain Framework for IoT-EHRs Systems. *Procedia Comput. Sci.* **2018**, *141*, 159–166. [CrossRef]
60. Mishra, S.; Tyagi, A.K. Intrusion Detection in Internet of Things (IoTs) Based Applications using Blockchain Technolgy. In Proceedings of the 2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 12–14 December 2019; pp. 123–128.
61. Patil, A.S.; Tama, B.A.; Park, Y.; Rhee, K.H. A Framework for Blockchain Based Secure Smart Green House Farming. In *Lecture Notes in Electrical Engineering*; Springer Science and Business Media LLC: Berlin, Germany, 2017; Volume 474, pp. 1162–1167.
62. Lin, J.; Shen, Z.; Zhang, A.; Chai, Y. Blockchain and IoT based food traceability system. *Int. J. Inf. Technol.* **2018**, *24*, 1–16.
63. Dogo, E.M.; Salami, A.F.; Nwulu, N.I.; Aigbavboa, C.O. *Blockchain and Internet of Things-Based Technologies for Intelligent Water Management System*; Springer Science and Business Media LLC: Berlin, Germany, 2019; pp. 129–150.
64. Kamilaris, A.; Fonts, A.; Prenafeta-Boldύ, F.X. The rise of blockchain technology in agriculture and food supply chains. *Trends Food Sci. Technol.* **2019**, *91*, 640–652. [CrossRef]
65. Rejeb, A.; Keogh, J.G.; Treiblmaier, H. Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management. *Future Int.* **2019**, *11*, 161. [CrossRef]
66. Huckle, S.; Bhattacharya, R.; White, M.; Beloff, N. Internet of Things, Blockchain and Shared Economy Applications. *Procedia Comput. Sci.* **2016**, *98*, 461–466. [CrossRef]
67. Zhang, Y.; Wen, J. The IoT electric business model: Using blockchain technology for the internet of things. *Peer-To-Peer Netw. Appl.* **2016**, *10*, 983–994. [CrossRef]
68. Ruta, M.; Scioscia, F.; Ieva, S.; Capurso, G.; Di Sciascio, E. Regular research paper: Blockchain, Service-Oriented Architecture, Semantic Web of Things, Semantic Web. *J. Int.Things* **2017**, *3*, 46–61.
69. Huh, S.; Cho, S.; Kim, S. Managing IoT devices using blockchain platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea, 19–22 February 2017; pp. 464–467. [CrossRef]
70. Conoscenti, M.; Vetro, A.; De Martin, J.C. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6.

71. Lo, S.K.; Liu, Y.; Chia, S.Y.; Xu, X.; Lu, Q.; Zhu, L.; Ning, H. Analysis of Blockchain Solutions for IoT: A Systematic Literature Review. *IEEE Access* **2019**, *7*, 58822–58835. [CrossRef]
72. Abadi, F.A.; Ellul, J.; Azzopardi, G. The Blockchain of Things, Beyond Bitcoin: A Systematic Review. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1666–1672. [CrossRef]
73. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for Internet of Things. *Comput. Commun.* **2019**, *136*, 10–29. [CrossRef]
74. Thakore, R.; Vaghashiya, R.; Patel, C.; Doshi, N. Blockchain—Based IoT: A Survey. *Procedia Comput. Sci.* **2019**, *155*, 704–709. [CrossRef]
75. Ferrag, M.A.; Maglaras, L.; Janicke, H. Blockchain and Its Role in the Internet of Things. In *Strategic Innovative Marketing and Tourism*; Springer Proceedings in Business and Economics, Kavoura, A., Kefallonitis, E., Giovanis, A., Eds.; Springer: Cham, Switzerland, 2019; pp. 151–157. [CrossRef]
76. Dai, H.-N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A Survey. *IEEE Int. Things J.* **2019**, *6*, 8076–8094. [CrossRef]
77. Maroufi, M.; Abdolee, R.; Tazekand, B.M. On the Convergence of Blockchain and Internet of Things (IoT) Technologies. *J. Strat. Innov. Sustain.* **2019**, *14*, 1–11. [CrossRef]
78. Alamri, M.; Jhanjhi, N.Z.; Humayun, M. Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review. *Int. J. Comput. Sci. Netw. Secur.* **2019**, *19*, 244–258.
79. Lao, L.; Li, Z.; Hou, S.; Xiao, B.; Guo, S.; Yang, Y. A Survey of IoT Applications in Blockchain Systems. *ACM Comput. Surv.* **2020**, *53*, 1–32. [CrossRef]
80. Singh, J.; Michels, J.D. Blockchain as a Service (BaaS): Providers and Trust. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 23–27 April 2018; pp. 67–74.
81. Artificial Intelligence|Definition of Artificial Intelligence by Merriam-Webster. Available online: https://www.merriam-webster.com/dictionary/artificialintelligence (accessed on 24 April 2020).
82. Reddy, R. The challenge of artificial intelligence. *Comput. Long. Beach. Calif* **1996**, *29*, 86–98. [CrossRef]
83. Alzahrani, A.G.; Alenezi, A.; Atlam, H.; Wills, G.B. A Framework for Data Sharing between Healthcare Providers using Blockchain. In Proceedings of the 5th International Conference on Internet of Things, Big Data and Security (IoTBDS 2020), Prague, Czech Republic, 7–9 May 2020; pp. 349–358. [CrossRef]
84. Baldominos, A.; Saez, Y. Coin.AI: A Proof-of-Useful-Work Scheme for Blockchain-Based Distributed Deep Learning. *Entropy* **2019**, *21*, 723. [CrossRef]
85. Bilodeau, S. Massive Computing for Bitcoin Mining and AI. Available online: https://towardsdatascience.com/energy-smart-bitcoin-mining-dd7bd2d2a3fa (accessed on 8 October 2020).
86. Roman, R.; Zhou, J.; Lopez, J. On the features and challenges of security and privacy in distributed internet of things. *Comput. Netw.* **2013**, *57*, 2266–2279. [CrossRef]
87. Samaniego, M.; Jamsrandorj, U.; Deters, R. Blockchain as a Service for IoT. In Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 15–18 December 2016; pp. 433–436.
88. Atlam, H.F.; Walters, R.J.; Wills, G.B.; Daniel, J. Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT. *Mobile Net. Appl.* **2019**, 1–13. [CrossRef]
89. Alenezi, A.; Zulkipli, N.H.N.; Atlam, H.F.; Walters, R.J.; Wills, G.B. The Impact of Cloud Forensic Readiness on Security. In Proceedings of the 7th International Conference on Cloud Computing and Services Science, Porto, Portugal, 24–26 April 2017; pp. 539–545.
90. Atlam, H.F.; Alenezi, A.; Alharthi, A.; Walters, R.J.; Wills, G.B. Integration of Cloud Computing with Internet of Things: Challenges and Open Issues. In Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 21–23 June 2017; pp. 670–675. [CrossRef]

91. Ziegeldorf, J.H.; Matzutt, R.; Henze, M.; Grossmann, F.; Wehrle, K. Secure and anonymous decentralized Bitcoin mixing. *Future Gener. Comput. Syst.* **2018**, *80*, 448–466. [CrossRef]
92. Xu, R.; Chen, Y.; Blasch, E.; Chen, G. BlendCAC: A Smart Contract Enabled Decentralized Capability-Based Access Control Mechanism for the IoT. *Computers* **2018**, *7*, 39. [CrossRef]